symmetry

MDPI

Article

A Modulo Function-Based Robust Asymmetric Variable Data Hiding Using DCT

Sahib Khan [1], Khalil Khan [2], Arslan Arif [3], Muhammad Hassaballah [4], Jehad Ali [5], Qui Thanh Hoai Ta [6] and Lisu Yu [7,*]

1 Department of Telecommunication Engineering, University of Engineering and Technology Mardan, Mardan 23200, Pakistan; sahib.khan@polito.it
2 Department of Electrical Engineering, University of Azad Jammu and Kashmir, Muzaffarabad 13100, Pakistan; khalil.khan@ajku.edu.pk
3 Faculty of Engineering, University of Central Punjab, Lahore 54782, Pakistan; arslan.arif@ucp.edu.pk
4 Department of Computer Science, Faculty of Computers and Information, South Valley University, Qena 83523, Egypt; m.hassaballah@svu.edu.eg
5 Department of Computer Engineering and Department of AI Convergence Network, Ajou University, Suwon 16499, Korea; jehadali@ajou.ac.kr
6 Institute of Research and Development, Duy Tan University, Danang 550000, Vietnam; tathoaiqui@duytan.edu.vn
7 School of Information Engineering, Nanchang University, Nanchang 330031, China
* Correspondence: lisuyu@ncu.edu.cn

Received: 7 September 2020; Accepted: 3 October 2020; Published: 12 October 2020

Abstract: This work presents a new asymmetric data hiding technique that hides a variable number of secret message bits in the discrete cosine transform (DCT) coefficients of a cover image using a modular distance technique. Prior to data hiding, the proposed framework transforms a cover image from a spatial domain to various frequency coefficients using DCT. The DCT coefficients are arranged in two groups: one with low-frequency coefficient, and the other with the medium and high-frequency coefficients. The medium and higher frequency coefficients are processed for variable data hiding asymmetrically. The proposed technique hides variable sets of secret information bits in different coefficients. The variation in hidden secret information is maintained using a key developed based on the modulo of distance of a coefficient from the reference point. The same key is also used to retrieve the confidential information at the receiver ends. The results reveal that the presented framework does not create any visually significant distortion, and thus the hidden information does not attract the human visual system (HVS). The technique also results in high data hiding efficiency.

Keywords: asymmetric data hiding; modulo function; DCT; *PSNR*; *SSIM*; hiding efficiency

1. Introduction

The advancement in technology has brought a revolution in computer and Internet technology. The use of the Internet has increased many fold with the availability of high-speed Internet and economical hardware. Along with the development of technology, the use of social media has increased. This technology has created several problems and fueled the development of information security on top of these problems along with positive features. The researchers are developing new techniques to ensure the

security of information and restrict unauthorized users' access to information. For increasing the security of hidden information, several cryptographic and data hiding techniques have been proposed [1,2].

In cryptography, the secret information is encrypted using an encryption key. The plain data (unencrypted data) is converted into cipher data (encrypted data) using encryption algorithms and the key. The encryption process changes the shape of the original information. The changes made in encrypted information are easily detectable. However, it is not easy to get the initial information without having the key. Therefore, the key plays an essential role in the security of the data. An efficient and robust cryptography technique has a large key size and provides a high level of protection.

In contrast to cryptography techniques, data hiding techniques do not change the original secret message; instead, they hide a secret message in other media called cover media [3,4]. The information is hidden innocently, and the presence of the hidden message remains unpredictable and undetectable to HVS [5]. Data hiding has received much attention due to security issues over the Internet. Usually, either cryptography or data hiding is used to secure information and secret messages. However, some forensics applications have used data hiding and cryptography and proposed several hybrid models with enhanced security.

Data hiding processes secret message bits and embed the secret message in a cover media. The possible cover medium used for data hiding includes text, audio, image, and video. The techniques used for data hiding techniques are classified in various categories based on the type of cover media used. Each cover media has its importance and plays an essential role in securing secret information using data hiding techniques. However, the cover medium with a high level of redundancy is considered much suitable for information hiding. Due to the high redundancy level of the digital image is widely used as a cover medium to accommodate secret data and transmit confidential information. Besides secure communication and information hiding, data hiding has other exciting applications, e.g., watermarking, copyright protection, data integrity assurance, and authentication of contents [6,7].

An image data hiding technique is implemented either in the spatial domain using image pixels directly or in the transform domain using transform coefficients. In the spatial domain, secret information is hidden in the least significant bits (LSBs) of image pixels, while in the transform domain, the coefficients of transformation are used to embed secret data. In the DCT domain, the DCT coefficients are used for information hiding, and the LSBs of the coefficients are replaced with the secret message bits. Similarly, the discrete wavelet transform (DWT) coefficients are used to accommodate secret data inside it by replacing the LSB of the DWT coefficient with the bits of secret information. After hiding information, the stego image is obtained with hidden information inside it. The spatial domain techniques directly result in stego images, while in the transform domain, the modified transform coefficients cover image are converted back by taking the inverse transform.

This paper presents a novel image data hiding technique in the transform domain, where the DCT coefficient of the cover image is used as media. The proposed method hides a different number of secret message bits in the LSBs of DCT coefficients of the cover image under test. The technique applies DCT to a cover image and gets an array of DCT coefficients. The DCT coefficients are classified into two groups. The group of low-frequency coefficients, having maximum energy of the image, and another group contains medium and high-frequency components. The low-frequency coefficients are not modified, while the rest of DCT components are subjected to hiding, and secret message bits are embedded in these components using the proposed framework. Different frequency coefficients are processed for information hiding using variable LSBs substitution mechanisms. The variation of the hidden information is achieved with the help of a modular distance technique (MDT) using a stego key. The stego key contains the information details of the number of hidden bits in different DCT coefficients. The stego key plays an essential role in the retrieval process. That is why it is kept secret and shared only with the intended party through a trusted third-party.

The rest of the paper is organized as follows. Section 2 presents the related work. The implementation of the proposed technique is presented in Section 3. Section 4 presents the details of the experiments performed, the results obtained, and analysis of the result. Comparison of the proposed technique with previous data hiding methods is presented in Section 5, and finally the paper is concluded in Section 6.

2. Related Work

This section presents a brief review of both the spatial and transform domains' image data hiding techniques. The first couple of data hiding techniques were introduced by Honsinger et al. and Fridrich et al. [8,9]. The methods used the LSBs of the cover image and embedded fixed amount of secret data per pixel. These techniques resulted in high-quality stego images; however, the hidden information can be recovered quickly, due to fixed data hiding, if its presence is suspected.

Lin et al. [10] used compressed images for information hiding. They proposed utilizing a prediction technique and judgment process to efficiently choose the embeddable blocks in data hiding, extraction, and recovery stages. At the end of image compression, the processed image was used for watermarking and steganography [11,12].

A framework for information hiding was introduced by hiding secret data in the edges of cover images only and preserving the rest of image quality and leaving the smooth region element unmodified. This set of data hiding methods includes LSB methods [13], side-match methods [13,14], PVD-based methods, and other techniques [15,16]. Besides the good quality of resulting stego images, these methods have a very minimal and small hiding capacity [14,17–19]. A new technique with high data hiding capacity was proposed in [20] to hide secret messages in the pixels that belong to edges. The complex region is isolated from the smooth region using the ACO algorithm [21,22]. The ACO-based complex region detection framework [18] is used for data hiding in combination with the 4LSB data hiding mechanism.

The spatial domain data hiding techniques discussed hide a fixed number of bits either in all pixels of a cover image or in the pixels that belong to the complex region. To further enhance the protection level of secret information, a set of techniques were proposed, hiding variable number secret information bits in the LSBs cover images. This idea was initially used in [23] for information hiding using random LSB of the cover image for hiding the secret message. A set of new techniques were presented in [24–26] to hide variable amounts of secret data in the LSBs of the cover medium pixels.

Along with the spatial domain, various data hiding methods were presented and implemented in the transform domain. A set of reversible data hiding techniques using DCT include data hiding schemes proposed by Iwata et al. [27], Chang et al. [28], Lin and Shiu [29], and Lin et al. [30]. In [31,32], a framework for data hiding was proposed. This method used DCT and singular value decomposition (SVD) collectively for information hiding [31,32]. They recommend a watermarking framework based on DCT, DWT, and SVD. They divided the image into four quadrants using a zigzag series after applying DCT. Then each quadrant is processed using SVD to adjust the watermark. The algorithm resulted in high quality of images and proved robust to various attacks. In [33,34], the authors used all four frequency bands of DWT combined SVD for watermarking. The experimental results show that Lin et al.'s method [30] gives the best magnitude of wavelet coefficient and singular values [35,36].

In [33], a block matching approach was used for the data hiding technique using DWT. In [29], a random key-based data hiding technique is proposed. The idea of stream cipher linear-feedback shift register (LFSR) is used for random key generation. Another method of data hiding in RGB images can be found in [37]; it combines the matrix pattern (MP) and LSB substitution techniques. Various forensics experts explore several other data hiding techniques, and they presented some very efficient steganographic methods that improved the security of the hidden information. In [38], data hiding is presented using two quantization levels of each block of AMBTC using Hamming codes. However, the distortion error of the

technique is relatively large. Kingsley and Barmawi [39] proposed a code-based data hiding technique using multiple embedding framework. Further details of the steganographic techniques can be found in [40,41].

3. The Proposed Technique

The proposed technique hides the bits of secret message in the LSBs of the DCT coefficient of a cover image in an asymmetric manner, i.e., hiding the different number of bits in different coefficients. The proposed method is an inspiration from the VTVB data hiding technique [42]. The proposed technique and VTVB data hiding technique hides a variable amount of secret data in DCT coefficients using a $Stego_{Key}$. However, then the proposed technique is different from VTVB data hiding in several aspects. First, the VTVB data hiding technique hides secret message bits in all DCT coefficients, i.e., low-, medium, and high-frequency coefficients, which creates a blurring effect stego image.

Moreover, the proposed technique excludes the lower frequency coefficient of DCT, enhancing the quality of the stego image. Other differences are the stego key and using the $Stego_{Key}$ for data hiding. The VTVB technique considers a $2D$ array of the DCT coefficients. VTVB then hides secret data by processing the DCT coefficients row by row. The $Stego_{Key}$ is initialized at the beginning of each row, which is the VTVB technique's weakness. An intruder will target only the first block of coefficients of each row of DCT array to crack the algorithm. The proposed technique does not initialize the $Stego_{Key}$ for each row, instead, it uses the DCT coefficient arranged in a vector. The other problem with the VTVB data hiding technique is when the number of DCT array columns is not completely divisible by the size of $Stego_{Key}$. For example, if the number of columns in a DCT array is 100 and the $Stego_{Key}$ size is 15, the key will completely cover the first 90 coefficients of each row. In each row, we are left with 10 coefficients and 15 $Stego_{Key}$ elements. What will be the solution to this problem? The VTVB technique is silent about this. This also creates a problem during the recovery of the secret data, and even the authorized person cannot recover secret data.

In contrast, the proposed technique does not suffer from this problem as it arranges DCT coefficients in a $1D$ vector. The generation and organization of the proposed technique's $Stego_{Key}$ are also different from the VTVB technique. The proposed technique has solved the problem of VTVB data hiding techniques.

To hide secret message bits in the DCT coefficient of a cover image. Initially, a cover image under test is processed using DCT, and an array of DCT coefficients is obtained. As we know that most of the energy of an image exists in the low-frequency components of the DCT array, any modification made in high-energy component creates relatively higher distortion. The high energy components, i.e., lower frequency coefficients of DCT array, are not used for information hiding. Therefore the DCT coefficients are classified into two groups—the group of low-frequency coefficients and other groups of medium and high-frequency coefficients. The medium and high-frequency coefficients of DCT array are used for information hiding. The frequency coefficients are subjected to variable data hiding, and different numbers of secret message bits are embedded in the different coefficients of the DCT array. The variable data hiding is implemented using the MDT framework.

The proposed technique is implemented using the following steps:

- DCT coefficients extraction
- Classification of DCT coefficients
- VTVB [42] data hiding using MDT
- Information retrieval

Each of these steps is explained with detail in the subsequent sections.

3.1. DCT Coefficients Extraction

DCT performs a real transformation to convert actual data points into its real spectrum to avoid redundancy. Using the proposed technique for secret information concealing the cover image under consideration is processed using DCT transform to cover the images into statistically independent coefficients. The interdependencies among the coefficient are removed to gain insight into the image details such as edges, energy, ... etc. It also makes the separation of the high energy coefficients from the rest of the coefficients very easy [43].

Let us consider a cover image Cov having size $(R \times C)$, where R and C represent the number rows and columns, respectively. The cover image Cov processed using DCT transform and an array of DCT coefficient DCT_{coef} is obtained. The DCT_{coef} is of the same dimension as that of cover image Cov, i.e., $(R \times C)$. The DCT_{coef} is computed as expressed in Equation (1) [44].

$$DCT_{coef}(u,v) = c(u)c(v)\sum_{i=0}^{C-1}\sum_{j=0}^{R-1} Cov(i,j)cos\left[\frac{\pi u\,(2i+1)}{2C}\right] cos\left[\frac{\pi v\,(2j+1)}{2R}\right] \tag{1}$$

where

$$c(u)\begin{cases}\frac{1}{\sqrt{2}} & if\ u=0\\ 1 & otherwise\end{cases} \tag{2}$$

and

$$c(v)\begin{cases}\frac{1}{\sqrt{2}} & if\ v=0\\ 1 & otherwise\end{cases} \tag{3}$$

The DCT organized the frequency coefficient of an image in order of frequencies, placing the lower frequency coefficients first, and then higher frequency coefficients are placed in the array. The array of DCT coefficients has lower coefficients on the top left. The higher coefficients on the bottom right and the middle section of the array contain the medium frequency components.

3.2. Classification of DCT Coefficients

As discussed previously, the DCT coefficients are classified into two groups. Before classification, the DCT coefficients matrix is converted into vector DCT_z of size $L = R \times C$, using the zigzag pattern as expressed in Equation (4).

$$DCT_z = ZigZag\left(DCT_{coef}\right) \tag{4}$$

After, the arrangement of DCT coefficient in a single vector, the coefficient are classified in two groups; high-energy coefficients and low-energy coefficients. The classification is expressed in Equations (5) and (6).

$$DCT_{Lcoef} = DCT_z\,(i)\ \text{ if } 1 \le i \le 0.25L \tag{5}$$

$$DCT_{Rcoef} = DCT_z\,(i)\ \text{ if }\ 0.25L < i \le L \tag{6}$$

Here, it is important to mention that 25% of low-frequency coefficients are assigned to the group of high-energy frequency coefficients' group, while the rest of 75% coefficient are assigned to the second group and are used for data hiding.

3.3. Data Hiding

The data hiding process is initiated after the successful classification of DCT coefficients. The data hiding process is performed based on the key ($Stego_{Key}$). The $Stego_{Key}$ defines the number of secret bits that

are hidden in a particular DCT coefficient. The $Stego_{Key}$ ensures the hiding algorithm's asymmetry and plays a vital role in retrieving the hidden information. Based on the $Stego_{Key}$, a different number of secret message bits are hidden in different coefficients. The variation in the amount of data bits hidden in various DCT coefficients is achieved with the MDT algorithm and the $Stego_{Key}$. The MDT algorithm ensures the variability of the hidden bits and protects information in the DCT coefficients in the following manner.

The MDT algorithm takes the DCT_{Rcoef} vector and selects a reference coefficient, let say (r). Then, each of the coefficients in the array is processed for data hiding one by one. The distance dm between the reference point and the DCT coefficient under test $DCT_{Rcoef}(j)$ is computed using the Euclidean distance method as expressed in Equation (7).

$$dm(j) = |r - j| \tag{7}$$

Then, a number called pattern factor P_f is used. The value of P_f is equal to the size of $Stego_{Key}$. It is used to determine the pattern of variation of the number of bits used for data hiding. P_f is the number of DCT coefficients, after which the number bits used for data hiding are repeated. After setting the P_f, the other factor m is computed as expressed in Equation (8).

$$m = mod\left(dm(j), P_f\right) \tag{8}$$

where the function $mod(.)$ is called the modulo operation and returns the remainder after division. The factor m is responsible for deciding the number of bits to be hidden in a coefficient, and it also set the size of the $Stego_{Key}$. The higher the value of m the larger the size of $Stego_{Key}$, and therefore the more secure the information is. The large key size makes it difficult to break the data hiding technique and retrieve the hidden information. A sample $Stego_{Key}$ of the proposed technique is presented in Equation (9).

$$Stego_{Key} = \{b_0, b_1, b_2, \ldots, b_m\} \tag{9}$$

After deciding the factor P_f, computing m, and fixing the $Stego_{Key}$, the information hiding process starts. The hiding process results in a vector of modified DCT coefficients called stego DCT coefficient $Steg_{DCT}$. The $Steg_{DCT}$ is of the size as that of DCT_{Rcoef}. The data hiding process is expressed in Equation (10).

$$Steg_{DCT}(i) = DH\left(DCT_{Rcoef}(i), B_j\right) \ where\ |B_j| = b_j \ \ \& \ \ 0 \leq j \leq m \tag{10}$$

where $DH(.)$ is the data hiding function that hides secret data bits in the LSBs of the selected DCT coefficients, the data hiding function $DH(.)$ uses an LSB substitution mechanism for replacing the LSBs of the selected DCT coefficients with secret data bits. $DCT_{Rcoef}(i)$ and $Steg_{DCT}(i)$ represent the ith coefficient of DCT_{Rcoef} and $Steg_{DCT}$ vectors, respectively. The B_j represents a set of secret message bits selected as the jth element of the $Stego_{Key}$, i.e., b_j. The suffix i represents the ith DCT coefficient subjected to data hiding and j is the index of the jth element of the $Stego_{Key}$.

Finally, a stego image is obtained by taking the inverse DCT of the modified coefficients. That is $Steg_{DCT}(i)$, as expressed in Equation (11).

$$Steg_{image} = IDCT\left(Steg_{DCT}\right) \tag{11}$$

Implementation of the porposed technique is summarized in the block diagram presented in Figure 1.

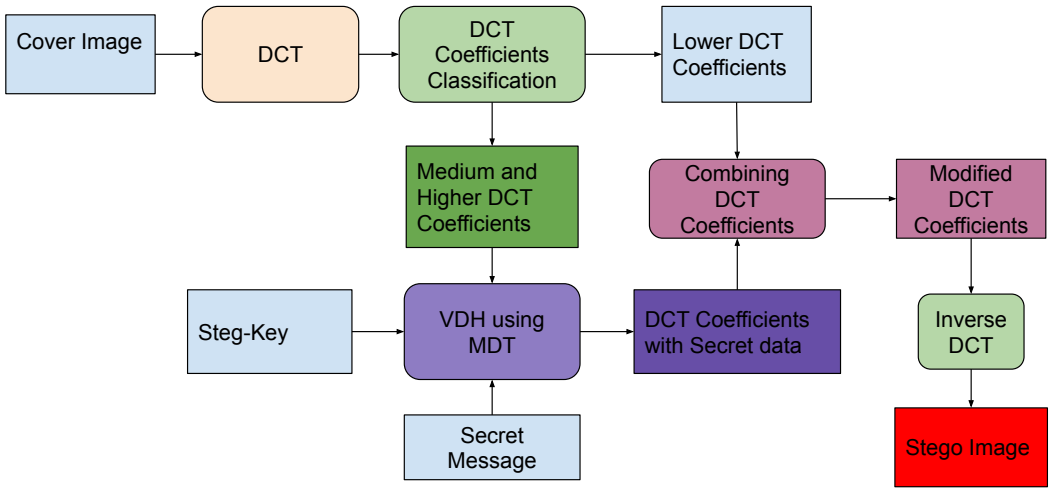


Figure 1. Block diagram of modulo function based robust asymmetric variable data hiding technique using DCT.

The stego image $Steg_{image}$ is compared with the original cover image Cov by computing the quality measuring parameters (e.g., $PSNR$ and $SSIM$). The same evaluation metrics and hiding capacity are used to compare the proposed technique with previous work.

3.4. Information Retrieval

Hiding secret data in the DCT coefficient of the cover image is an important operation performed on the source side. Along with hiding, it is also important to retrieve all the hidden information efficiently with full strength. Information retrieval is a process that ensures the 100% recovery of hidden information of the receiver side. The proposed data hiding technique is reversible, and the reverse process can be used to retrieve the hidden information. To retrieve the information hidden using the proposed framework, we need to perform DCT some prior step of the data hiding process, i.e., DCT coefficients extraction and classification of the DCT coefficients.

For retrieving the hidden information, DCT transform is applied to the stego image $Steg_{image}$, as expressed in Equation (12).

$$Steg_{dct-coef} = DCT\left(Steg_{image}\right) \tag{12}$$

The array of DCT coefficients $Steg_{dct-coef}$ is converted into a vector of the DCT coefficient using the zigzag scanning approach, as expressed in Equation (13).

$$Steg_{dct-vec} = ZigZag\left(Steg_{dct-coef}\right) \tag{13}$$

The DCT coefficients in the vector $Steg_{dct-vec}$ are classified into two groups, i.e., low-frequency coefficient group and group consist medium and high-frequency coefficients, as expressed in Equations (5) and (6), respectively. The group of DCT coefficients, consisting of the medium and high-frequency coefficient, has hidden information. These coefficients are processed for information retrieval. The stego key, i.e., $Stego_{Key}$, plays an important role at this stage. Without the $Stego_{Key}$, it is not impossible to retrieve the hidden information. All the DCT coefficients are processed for computing the factor m, processing one coefficient at a time. The $Stego_{Key}$ and m, both are used to retrieve the hidden information. The hidden information is retrieved by extracting the LSB of the DCT coefficients, using the

$Stego_{Key}$ and m. This process ensures the 100% recovery of the hidden information. The retrieval process is presented in Figure 2.

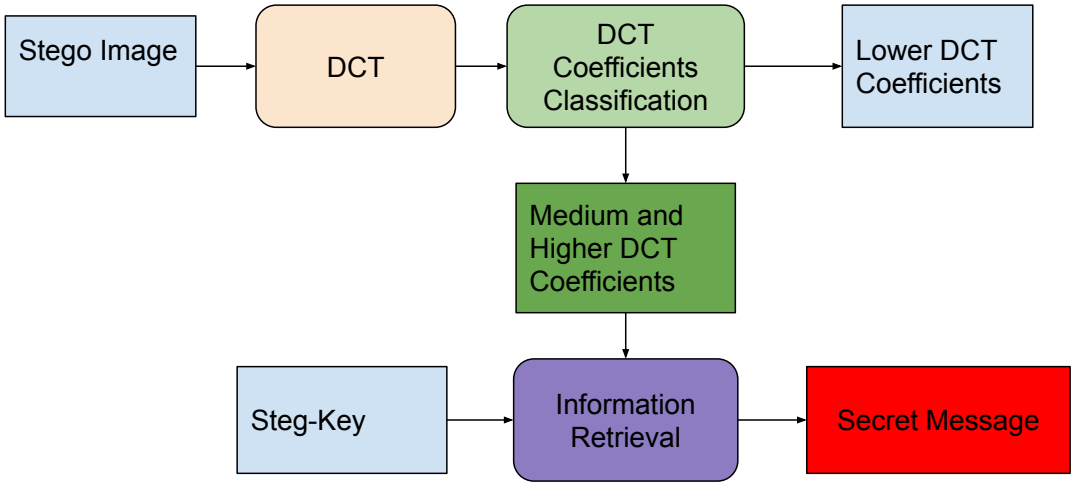


Figure 2. The process of information retrieval.

3.5. Evaluation Metrics

The proposed data hiding technique's performance is measured and analyzed using the evaluation measure of hiding capacity (HC), and peak signal to noise ratio ($PSNR$) and structural similarity ($SSIM$). The HC and $PSNR$ are defined by Equations (14) and (15), respectively [45].

$$HC = \left(\frac{Total\ Bits\ Hidden}{R \times C \times 8} \right) \times 100 \tag{14}$$

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \tag{15}$$

where MSE is the mean square error and is given as

$$MSE = \frac{\sum_{i=1}^{R} \sum_{j=1}^{C} \left(Cov\,(i,j) - Steg_{image}\,(i,j) \right)^2}{R \times C} \tag{16}$$

The $SSIM$ [46] is mathematically expressed as

$$SSIM(Cov, Steg_{image}) = \frac{\left(2\mu_{Cov}\mu_{Steg_{image}} + C_1\right)\left(2\sigma_{Cov\ Steg_{image}} + C_2\right)}{\left(\mu_{Cov}^2 + \mu_{Steg_{image}}^2 + C_1\right)\left(\sigma_{Cov}^2 + \sigma_{Steg_{image}}^2 + C_2\right)} \tag{17}$$

where μ_{Cov} is the mean of Cov, $\mu_{Steg_{image}}$ is the mean of $Steg_{image}$, σ_{Cov}^2 is the variance of Cov, $\sigma_{Steg_{image}}^2$ is the variance of $Steg_{image}$, $\sigma_{Cov\ Steg_{image}}$ is the covariance of Cov and $Steg_{image}$, C_1 and C_2 are the factors used to stabilize the division with weak denominator.

The hiding capacity HC of the proposed method depends on the number of bits hidden in different coefficients, which is defined by $Stego_{Key}$. Similarly, the $PSNR$ and other quality measuring parameters also depend on the amount of data hidden in the cover image. Hiding more data in DCT components increases HC; however, it creates more distortion. The distortion may become significant with an extensive

hiding data in the cover image. For an efficient data hiding technique, the stego image quality should be higher than 30 dB in terms of $PSNR$.

4. Experimental Results and Analysis

The performance of the proposed technique is analyzed using different experiments. Initially, one cover image called Building, as given in Figure 3, is used for experiments. The cover images are used for information using the proposed technique and using different sego keys.

Figure 3. Cover Image: Building.

Before data hiding, the DCT is applied to the cover image in Figure 3, and the array of DCT coefficients are computed. The DCT coefficients are classified as discussed in the Section 3.2. The high-energy coefficients, i.e., the low-frequency components, are left unaffected. The low-energy components, i.e., medium and high-frequency components, are processed for data hiding using $Stego_{Key}$ of different sizes, as discussed in Section 3.3.

In the first experiment, the medium and high DCT coefficients of the cover image are subjected to data hiding using the proposed method, with a key size equal to 2. The key used is given as

$$Stego_{Key} = \{1, 2\}. \tag{18}$$

Only two different numbers of bits are used for embedding purposes. After hiding information in the selected DCT coefficients, the modified DCT coefficients are processed with IDCT transform to get a stego image. The stego image obtained is shown in Figure 4.

The resulting stego image shows that for the given key proposed algorithm creates a high-quality stego image. It also shows that the presence of hidden information is not detectable to HVS. Therefore, the proposed technique can be used for the secure exchange of secret data.

Figure 4. The stego image obtained with $Stego_{Key}$ of size 2 using the proposed technique.

The experiment is repeated using the medium and high DCT coefficients of the same cover image. The DCT coefficients are subjected to data hiding using the proposed technique, with a key size equal to 3. The used key is

$$Stego_{Key} = \{1, 2, 3\}. \tag{19}$$

The resulting stego image is illustrated in Figure 5 and it shows that the given key proposed algorithm also creates a high-quality stego image and keeps hidden information undetectable to humans.

Figure 5. The stego image obtained with $Stego_{Key}$ of size 3 using the proposed technique.

In the third experiment, a key of size 4 is used to hide secret information in the medium and high DCT coefficients of the same cover image. Secret information is hidden in the DCT coefficients. The $Stego_{Key}$ is

$$Stego_{Key} = \{1, 2, 3, 4\}. \tag{20}$$

The resulting stego image is shown in Figure 6. It shows that the given key proposed algorithm also generates a high-quality stego image.

Figure 6. The stego image obtained with $Stego_{Key}$ of size 4 using the proposed technique.

The experiment is repeated with a key of size 5, and information is embedded in the selected group of DCT coefficients of the same cover image, where the used key in this case is

$$Stego_{Key} = \{1, 2, 3, 4, 5\}. \tag{21}$$

The resulting stego image having good visual quality is shown in Figure 7.

Using the medium and high-frequency coefficients of the cover image in Figure 3, the experiment is repeated for $Stego_{Key}$ of size 6 and 7. The stego keys of size 6 and 7 are expressed in Equations (22) and (23), respectively.

$$Stego_{Key} = \{1, 2, 3, 4, 5, 6\}. \tag{22}$$

$$Stego_{Key} = \{1, 2, 3, 4, 5, 6, 7\}. \tag{23}$$

Each of the keys is used to hide secret information in the DCT coefficients and the stego image is obtained for each experiment. The stego images generated with $Stego_{Key}$ of size 6 and 7 are given in Figures 8 and 9, respectively.

Figure 7. The stego image obtained with $Stego_{Key}$ of size 5 using the proposed technique.

Figure 8. The stego image obtained with $Stego_{Key}$ of size 6 using the proposed technique.

Figure 9. The stego image obtained with $Stego_{Key}$ of size 7 using the proposed technique.

The results show that both of these keys of size 6 and 7, generate high-quality stego images. The hidden data does not attract the attention of HVS and therefore keeps the existence of hidden information blind to intruders.

Along with stego images, the performance of the proposed algorithm is evaluated quantitatively by computing HC, $PSNR$, and $SSIM$. The evaluation metrics are obtained for each experiment performed with stego keys of different sizes, (2, 3, 4, 5, 6, and 7). The results obtained are listed in Table 1.

Table 1. The resulting HC, $PSNR$, and $SSIM$ of the proposed technique with $Stego_{Key}$ of different sizes.

	Evaluation Metrics		
Key Size	***HC* (%)**	***PSNR* (dB)**	***SSIM***
2	12.2743	48.23	0.9893
3	12.2743	48.23	0.9893
4	24.5486	39.98	0.846
5	18.4115	45.75	0.9568
6	12.2743	48.23	0.9893
7	12.2743	48.23	0.9893

These results prove that the proposed algorithm can hide secret information with high hiding efficiency. The results indicate that for the given keys as the key size increase from 2 to 4, the hiding capacity increases from 12.2743% to 24.5486% and with further increase in key size as a reduction in hiding capacity occurs. Similarly, looking into the results obtained in terms of $PSNR$ and $SSIM$, the quality of stego images increases and decreases with an increase or decrease in hiding capacity, respectively.

Here, it is important to mention that it is not crucial to have a monotonic increase in the number of bit in a stego key. The number of bits can be arranged in any order, and any value from 0 to 8 can be used. For example, we can use a key of size 25, given in Equation (24), with a different number of bits to be hidden in different DCT coefficients.

$$Stego_{Key} = \{0, 2, 4, 5, 8, 3, 4, 6, 9, 2, 7, 8, 3, 6, 8, 1, 0, 8, 4, 3, 1, 7, 4, 2, 5\} \tag{24}$$

In the last part of experimentation, a single cover image, Building for data hiding with different $Stego_{Key}$s. For evaluating a data hiding technique, single image experimentation and results are not enough to prove and justify the effectiveness of performance compared with other state-of-the-art techniques. Therefore, the data hiding technique's performance is further evaluated using different cover images, e.g., Cameraman, Jelly Beans, Lena, Mandrill, Pepper, and Tiffany, shown in Figures 10a–15a, respectively.

The cover images are processed for data hiding using the proposed method with stego key of size 7. Where

$$Stego_{Key} = \{1, 2, 3, 4, 5, 6, 7\}. \tag{25}$$

The resulting stego images are shown in Figures 10b–15b, respectively.

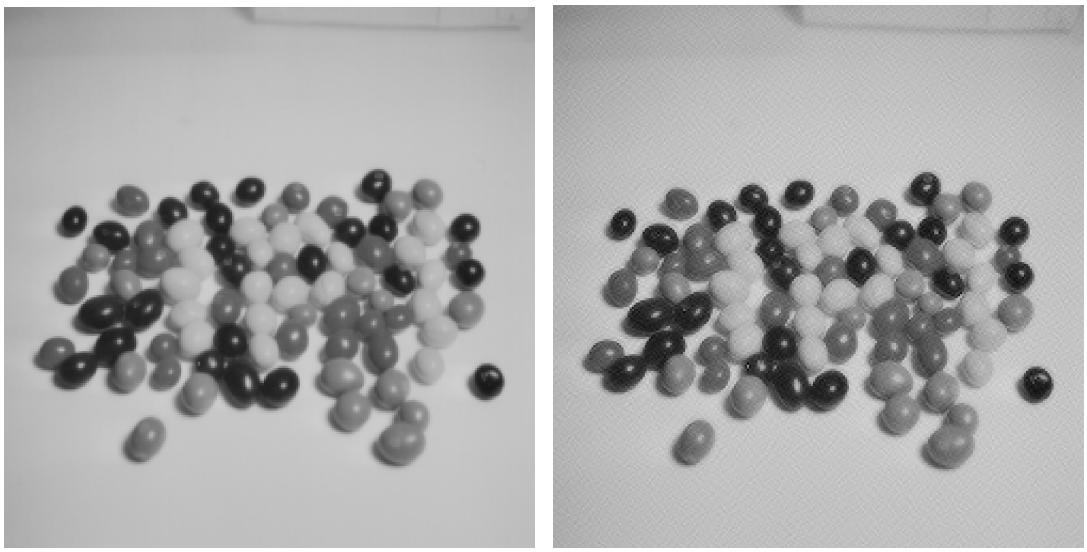
The cover Figure 10a, is subjected to data hiding stego image with hidden information inside it is obtained. The resulting stego image in Figure 10b, showing the proposed technique generates a high-quality stego image, and the quality of the stego image is almost the same as that of the original cover image. There is no visually compelling distortion present in the stego image. Therefore, the proposed technique is equally effective in the Cameraman image.

(**a**) (**b**)

Figure 10. Results obtained for Cameraman with $m = 7$. The proposed technique with key size 7 used to hide information in the Cameraman image (**a**) and the stego image (**b**).

The Jelly Beans image, the cover Figure 11a is subjected to data hiding with the same key size of 7, and the stego image with hidden information inside it is obtained as shown in Figure 11b.

The resulting stego image shows the proposed technique also generates high-quality stego images using Jelly Beans images as cover. The quality of the stego image is similar to the original cover image. There is no visually compelling distortion present in the stego image. Therefore, the proposed technique is equally effective in the Cameraman image.



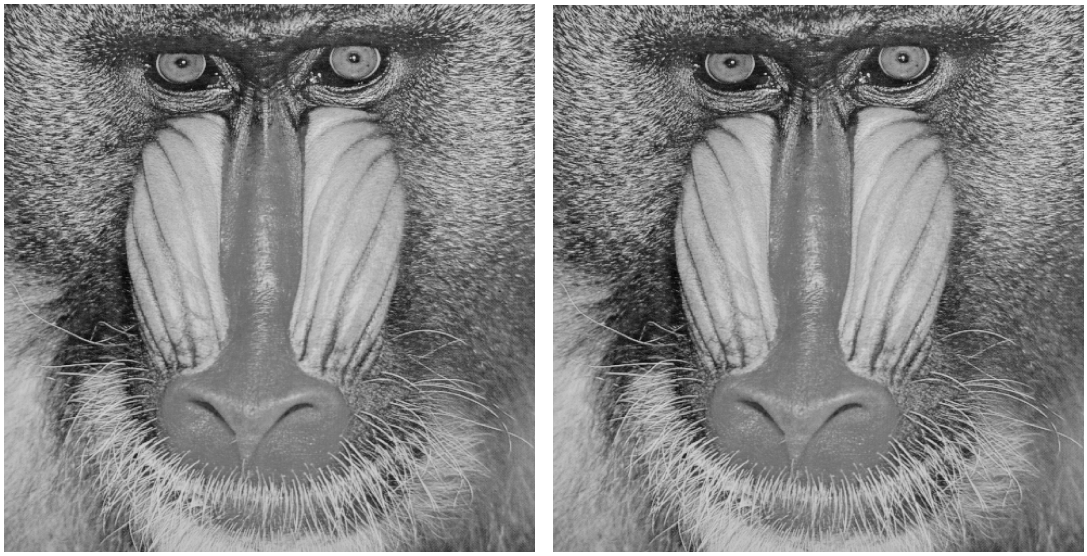
(**a**) (**b**)

Figure 11. Results obtained for Jelly Beans with $m = 7$. The proposed technique with key size 7 used to hide information in the Jelly Beans image (**a**) and the stego image (**b**).

(**a**) (**b**)

Figure 12. Results obtained for Lena with $m = 7$. The proposed technique with key size 7 used to hide information in the Lena image (**a**) and the stego image (**b**).

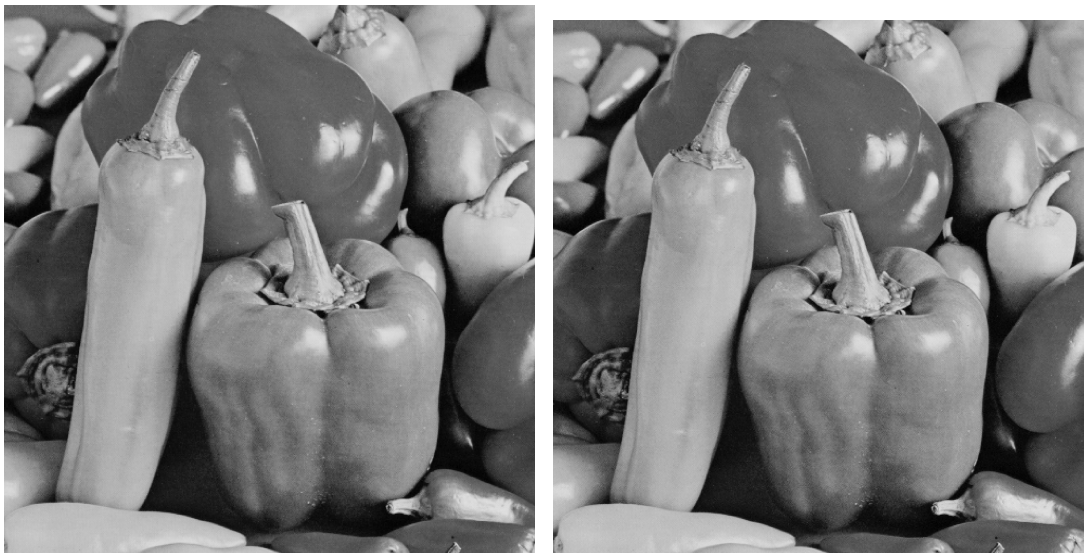
Similarly, the experiment is repeated for the rest of the images, i.e., Lena, Mandrill, Pepper, and Tiffany. Each image is used as a cover image one by one, and information is hidden in selected DCT coefficients of the cover images. The stego key of size 7 is also used in each of the experiments. The cover images and corresponding stego images are shown side by side to make a better qualitative analysis. The result shows that the proposed technique generates good quality stego image in each of the experiments.



(**a**) (**b**)

Figure 13. Results obtained for Mandrill at $m = 7$. The proposed technique with key size 7 used to hide information in the Mandrill image (**a**) and the stego image (**b**).

Qualitative analysis shows that the hidden information does not contribute any significant distortion using the proposed technique. The quality of each of the resulting stego images resembles that of the original one. Therefore, the hidden information does not attract the intruders' attention and is considered safe. From all the results, it can be concluded that the proposed technique is an efficient data hiding and is a new contribution to the field of data security.



(**a**) (**b**)

Figure 14. Results obtained for Pepper with $m = 7$. The proposed technique with key size 7 used to hide information in the Pepper image (**a**) and the stego image (**b**).

(**a**) (**b**)

Figure 15. Results obtained for Tiffany with $m = 7$. The proposed technique with key size 7 used to hide information in the Tiffany image (**a**) and the stego image (**b**).

The quantitative results obtained for the different cover images are listed in Table 2. The results show that the proposed technique has a hiding capacity of around 12% for all the different cover images. While the $PSNR$ of the proposed technique is also very high, a maximum $PSNR$ of 48.82 dB is obtained using Mandrill as a cover image. Similarly, the values of $SSIM$ obtained on different images are very high and remain above 0.9 for the cover images except for Jelly Beans. The $SSIM$ obtained for the Jelly Beans image is slightly lower than the other and is equal to 0.8709.

Table 2. The resulting HC, $PSNR$, and $SSIM$ of the proposed technique with $Stego_{Key}$ of size 7 using different cover images.

	Evaluation Metrics		
Cover Image	***HC* (%)**	***PSNR* (dB)**	***SSIM***
Cameraman	12.3749	48.23	0.9733
Jelly Beans	12.8395	35.54	0.8709
Lena	12.291	46.05	0.9909
Mandrill	12.291	48.82	0.9972
Pepper	12.291	47.17	0.9915
Tiffany	12.291	46.15	0.9901

Along with the high-quality stego image and large HC, the proposed technique strength and robustness against different steganalysis and cracking technique is also analyzed. The proposed technique is tested against different steganalysis attacks using StegExpose [47], StegSecret [48], and Jia-Fa method [49]. The experimental results revealed that the proposed technique is robust against spatial and DCT domain steganalysis attacks.

5. Comparison

A steganographic technique aims to ensure the security of secret information by hiding it in some cover medium. Several steganographic techniques are available in the literature. The selection of a suitable

steganographic method, among the possible, is essential and plays a vital role in achieving excellence in information security. A proper steganographic technique has a high capacity to hide without affecting the quality of resulting stego images.

This section compares the proposed data hiding technique with state-of-the-art data hiding methods. The comparison is made based on hiding capacity HC, peak signal to noise ratio $PSNR$, and structure similarity index $SSIM$. The proposed technique is compared with well-know data hiding techniques of Honsinger et al. [9], Macq and Dewey [50], Fridrich et al. [8], Lin and Li [51], Jaiswal et al. [52], Goljan et al. [53], Vleeschouwer et al. [54], Khan et al. [55], Alam et al. [56], Wang et al. [57], Khan and Tiziano [20], Khamrui and Mandal [58], Chang et al. [28], Lee and Chen [59], Lin and Shiu [29], Koikara and Goswami [60], Hou et al. [61], Wang et al. [62], and Huang et al. [63]. The comparison is made using three different cover images (Lena, Mandrill, and Pepper). The results obtained for each of the different data hiding techniques using Lena, Mandrill, and Pepper images are listed in Tables 3–5, respectively.

The results in Table 3 show that the proposed technique has a HC of 12.291%, which is higher than the most of the methods except for Wang et al. [57] and Lee and Chen [59] methods, which have higher HC than the proposed technique. The $PSNR$ of the proposed technique is also higher than or comparable with most of the methods except those of Alam et al., Lin and Li, and Wang et al. [62]. However, these three techniques have a lower HC than the proposed technique. Similarly, the $SSIM$ computed for the proposed technique is much higher than the rest of the methods. The overall analysis shows that the proposed technique has better or comparable performance with respect to the other data hiding techniques.

Table 3. A comparison of the proposed technique with other techniques using Lena image as cover.

Method	Evaluation Metrics		
	***HC* (%)**	***PSNR* (dB)**	***SSIM***
Honsinger et al.	<0.0156	-	-
Macq and Dewey	4.06	48.45	0.9891
Fridrich et al.	0.195	-	-
Lin and Li	0.0475	52.4572	0.9981
Jaiswal et al.	3.2875	48.7501	0.9754
Goljan et al.	4.5	39.00	0.9915
Vleeschouwer et al.	0.195	30.00	0.8662
Khan et al.	4.125	46.23	0.8771
Khamrui and Mandal	3.80	44.78	0.3050
Chang et al.	1.76	34.34	0.8542
Alam et al.	10.96	51.098	0.88
Wang et al. [57]	19.66	42.74	0.8796
Lee and Chen	50	39.58	0.8427
Lin and Shiu	2.75	33.80	0.8616
Koikara and Goswami	5.27	44.86	0.8274
Wang et al. [62]	0.55	53.51	0.9764
Huang et al.	0.38	47.12	0.9750
Hou et al.	0.39	47.3	0.9750
Proposed Technique	12.291	46.05	0.9909

The quantitative results obtained for different data hiding technique using Mandrill are listed in Table 4. The results show that the proposed technique also has a HC of 12.291% for Mandrill images. The HC of the proposed technique is higher than most of the methods except for Wang et al. [57] and Lee and Chen [59] method. The two techniques have HC higher than the proposed technique. The proposed technique has $PSNR$ higher than or comparable with the majority of the given technique.

In comparison, the data hiding techniques of Alam et al., Lin and Li, and Wang et al. [62] have higher $PSNR$ values than the proposed technique. However, the three techniques have lower performance than the proposed technique in terms of HC. Similarly, the computed $SSIM$ for the proposed technique is much better than the rest of these methods.

Table 4. A comparison of the proposed technique with other techniques using Mandrill image as cover.

Method	Evaluation Metrics		
	***HC* (%)**	***PSNR* (dB)**	***SSIM***
Honsinger et al.	<0.0156	-	-
Macq and Dewey	4.00	49.11	0.9889
Fridrich et al.	0.195	-	-
Lin and Li	0.0475	51.9255	0.9975
Jaiswal et al.	3.478	46.6210	0.9711
Goljan et al.	4.5	39.25	0.9931
Vleeschouwer et al.	0.195	31.51	0.8871
Khan et al.	4.5	46.05	0.8768
Khamrui and Mandal	3.82	45.83	0.3956
Chang et al.	1.79	34.94	0.8499
Alam et al.	11.20	50.88	0.8798
Wang et al. [57]	19.66	42.74	0.8796
Lee and Chen	50	39.58	0.8427
Lin and Shiu	3.15	26.75	0.8616
Koikara and Goswami	5.27	44.79	0.8274
Wang et al. [62]	0.78	53.60	0.9764
Huang et al.	0.36%	44.26 dB	0.9750
Hou et al.	0.35%	44.70 dB	0.9817
Proposed Technique	12.291%	48.82 dB	0.9972

Similar to Lena and Mandrill, the comparison is also made on using Pepper as a cover image. The quantitative results are shown in Table 5. The experimental results reveal that the proposed technique performs better than most of the techniques in terms of HC. Similarly, the proposed technique's performance is also better than, or comparable with, the majority of the techniques in terms of $PSNR$. However, the proposed technique has a lower $PSNR$ than the techniques of Alam et al., Lin and Li, Wang et al. [62], and Huang et al. using the Pepper image as cover media. However, the performance of the four techniques is lower and have lower HC than the proposed technique. Similarly, the $SSIM$ computed for the proposed technique is much higher than the rest of the methods. The overall analysis shows that the proposed technique has better or comparable performance with respect to the other data hiding techniques.

The experimental results show that the performance of the proposed technique is either better or comparable with the previous data hiding techniques performance, which shows the strength of the proposed technique. Furthermore, the proposed technique asymmetrically hides secret information by embedding different numbers of secret message bits in different DCT coefficients of the cover images and have a stego key of significantly large size, which further enhances the security of the hidden information. While the other techniques presented in the comparison section have fixed data hiding, it is easier to crack or break a data hiding technique with fixed data hiding. The high security of hidden information with large key size, high HC, $PSNR$, and $SSIM$ is the main strength of the proposed technique.

Table 5. A comparison of the proposed technique with other techniques using Pepper image as cover.

Method	Evaluation Metrics		
	***HC* (%)**	***PSNR* (dB)**	***SSIM***
Honsinger et al.	<0.0156	-	-
Macq and Dewey	3.81	49.25	0.9882
Fridrich et al.	0.195	-	-
Lin and Li	0.0475	51.4751	0.9975
Jaiswal et al.	3.274	48.9513	0.9762
Goljan et al.	4.5	39.02	0.9913
Vleeschouwer et al.	0.195	30.29	0.8650
Khan et al.	4.125	47.23	0.8854
Khamrui and Mandal	3.84	43.59	0.5250
Chang et al.	1.83	32.34	0.8446
Alam et al.	11.12	49.95	0.8775
Wang et al. [57]	19.66	42.74	0.8796
Lee and Chen	50	39.58	0.8427
Lin and Shiu	2.71	34.10	0.8616
Koikara and Goswami	5.27	44.83	0.8274
Wang et al. [62]	0.71	58.65	0.9764
Huang et al.	0.31	54.69	0.9750
Hou et al.	0.33	45.62	0.9738
Proposed Technique	12.291	47.17	0.9915

6. Conclusions

The proposed variable data hiding technique is a new approach for hiding secret messages in DCT coefficients of cover images. It uses medium and high-frequency coefficients for embedding secret data and hides the different amounts of confidential data in the various coefficients. The variable data hiding enhances the security of hidden information. Also, it has a flexible data hiding capacity and can be changed depending on the application by changing the stego key. Furthermore, the stego key of the proposed method is quite large and changeable. The large stego key strengthens the security further.

Along with high data hiding capacity and sizable key size, the proposed technique gives high-quality stego images. The hidden information does not introduce any visually significant distortion to the resulting stego images, and therefore keeps the existence of secret data invisible. The proposed technique can be used in different applications, such as the exchange of information in a secure manner, image steganography, watermarking, and secure data communication over Internet of things (IoT).

Author Contributions: All authors equally contributed in this research work. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Patani, K.; Rathod, D. Advanced 3-Bit LSB Based on Data Hiding Using Steganography. In *Data Science and Intelligent Applications*; Springer: Berlin, Germany, 2020; pp. 383–390.
2. Gurunathan, K.; Rajagopalan, S. A stegano-visual cryptography technique for multimedia security. *Multimed. Tools Appl.* **2020**, *79*, 3893–3911. [CrossRef]
3. Saxena, A.; Sinha, S.; Shukla, P. Design and development of image security technique by using cryptography and steganography: A combine approach. *Int. J. Image Graph. Signal Process.* **2018**, *10*, 1168–1175.

4. Sattar, I.; Gaata, M. Image steganography technique based on adaptive random key generator with suitable cover selection. In Proceedings of the 2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT), Baghdad, Iraq, 7–9 March 2017; pp. 208–212.
5. Sadat, E.S.; Faez, K.; Saffari Pour, M. Entropy-based video steganalysis of motion vectors. *Entropy* **2018**, *20*, 244. [CrossRef]
6. Johnson, N.; Jajodia, S. Exploring steganography Seeing the unseen. *Computer* **1998**, *31*, 26–34. [CrossRef]
7. Swanson, M.; Kobayashi, M.; Tewfik, A. Multimedia data-embedding and watermarking technologies. *Proc. IEEE* **1998**, *86*, 1064–1087. [CrossRef]
8. Fridrich, J.; Goljan, M.; Du, R. Invertible authentication. Security and Watermarking of Multimedia contents III. *Int. Soc. Opt. Photonics* **2001**, *4314*, 197–208.
9. Honsinger, C.; Jones, P.; Rabbani, M.; Stoffel, J. Lossless Recovery of an Original Image Containing Embedded Data. U.S. Patent US 6,278,791, 21 August 2001.
10. Lin, J.; Lin, C.C.; Chang, C.C. Reversible Steganographic Scheme for AMBTC-Compressed Image Based on (7, 4) Hamming Code. *Symmetry* **2019**, *11*, 1236.
11. Hong, W.; Ma, Y.B.; Wu, H.C.; Chen, T.S. An efficient reversible data hiding method for AMBTC compressed images. *Multimed. Tools Appl.* **2017**, *76*, 5441–5460. [CrossRef]
12. Shelupanov, A.; Evsyutin, O.; Konev, A.; Kostyuchenko, E.; Kruchinin, D.; Nikiforov, D. Information Security Methods—Modern Research Directions. *Symmetry* **2019**, *11*, 150. [CrossRef]
13. Guan, N.; Tao, D.; Luo, Z.; Yuan, B. NeNMF: An optimal gradient method for nonnegative matrix factorization. *IEEE Trans. Signal Process.* **2012**, *60*, 2882–2898. [CrossRef]
14. Hong, W.; Chen, T. A novel data embedding method using adaptive pixel pair matching. *IEEE Trans. Inf. Forensics Secur.* **2011**, *7*, 176–184. [CrossRef]
15. Hsu, C.; Tu, S. Probability-based tampering detection scheme for digital images. *Opt. Commun.* **2010**, *283*, 1737–1743. [CrossRef]
16. Subhedar, M.; Mankar, V. Current status and key issues in image steganography: A survey. *Comput. Sci. Rev.* **2014**, *13*, 95–113. [CrossRef]
17. Hong, W.; Chen, T.; Shiu, C. Reversible data hiding for high quality images using modification of prediction errors. *J. Syst. Softw.* **2009**, *82*, 1833–1842. [CrossRef]
18. Tian, J.; Yu, W.; Xie, S. An ant colony optimization algorithm for image edge detection. In Proceedings of the 2008 IEEE Congress on Evolutionary Computation (IEEE World Congress on Computational Intelligence), Hong Kong, China, 1–6 June 2008; pp. 751–756.
19. Jung, K.; Yoo, K. Data hiding using edge detector for scalable images. *Multimed. Tools Appl.* **2014**, *71*, 1455–1468. [CrossRef]
20. Khan, S.; Bianchi, T. Ant colony optimization (aco) based data hiding in image complex region. *Int. J. Electr. Comput. Eng. IJECE* **2018**, *8*, 379–389. [CrossRef]
21. Dorigo, M.; Thomas, S. *Ant Colony Optimization*; MIT Press: Cambridge, UK, 2004.
22. Duan, H. *Ant Colony Algorithms: Theory and Applications*, 1st ed.; Chinese Science: Beijing, China, 2005; ISSN 7-03-016204-8.
23. Kaur, D.; Verma, H.K.; Singh, R.K. *Image Steganography: Hiding Secrets in Random LSB Pixels*; Springer: Singapore, 2020; pp. 331–341.
24. Khan, S.; Yousaf, M.H.; Akram, J. Implementation of Variable Least Significant Bits Stegnography using DDDB Algorithm. *Int. J. Comput. Sci. Issues IJCSI* **2011**, *8*, 292–296.
25. Irfan, M.; Ahmad, N.; Khan, S. Analysis of Varying Least Significant Bits DCT and Spatial Domain Stegnography. *Sindh Univ. Res. J. SURJ Sci. Ser.* **2014**, *46*, 301–306.
26. Khan, S.; Ahmad, N.; Wahid, M. Varying index varying bits substitution algorithm for the implementation of VLSB steganography. *J. Chin. Inst. Eng.* **2016**, *39*, 101–109. [CrossRef]
27. Iwata, M.; Miyake, K.; Shiozaki, A. Digital steganography utilizing features of JPEG images. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2004**, *87*, 929–936.

28. Chang, C.; Lin, C.; Tseng, C.; Tai, W. Reversible hiding in DCT-based compressed images. *Inf. Sci.* **2007**, *177*, 2768–2786. [CrossRef]
29. Lin, C.; Shiu, P. DCT-based reversible data hiding scheme. In Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication, Suwon, Korea, 15–16 January 2009; pp. 327–335.
30. Lin, J.; Chen, Y.; Chang, C.; Hu, Y. Reversible data hiding in encrypted images based on bit-plane block embedding. *J. Inf. Hiding Multimed. Signal Process.* **2019**, *10*, 408–421.
31. AbdelWahab, O.; Hussein, A.; Hamed, H.A.; Kelash, H.M.; Khalaf, A.A.M.; Ali, H.M. Hiding data in images using steganography techniques with compression algorithms. *Telkomnika* **2019**, *17*, 1168–1175.
32. Yang, C.; Lin, Y. Fractal curves to improve the reversible data embedding for VQ-indexes based on locally adaptive coding. *J. Vis. Commun. Image Represent.* **2010**, *21*, 334–342. [CrossRef]
33. Kim, J.; Park, H.; Park, J. Image steganography based on block matching in DWT domain. In Proceedings of the 2017 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), Caligari, Italy, 7–9 June 2017; pp. 1–4.
34. Tseng, H.; Chang, C. High Capacity Data Hiding in JPEG-Compressed Images. *Informatica* **2004**, *15*, 127–142. [CrossRef]
35. Ganic, E.; Eskicioglu, A. Robust DWT-SVD domain image watermarking: Embedding data in all frequencies. In Proceedings of the 2004 Workshop on Multimedia and Security, Magdeburg, Germany, 20–21 September 2004; pp. 166–174.
36. El_Rahman, S. A comprehensive image steganography tool using LSB scheme. *Int. J. Image Graph. Signal Process.* **2015**, *7*, 10. [CrossRef]
37. Roy, S.; Venkateswaran, P. Online payment system using steganography and visual cryptography. In Proceedings of the 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science, Bhopal, India, 1–2 March 2014; pp. 1–5.
38. Kim, C.; Shin, D.; Yang, C.; Leng, L. Hybrid Data Hiding Based on AMBTC Using Enhanced Hamming Code. *Appl. Sci.* **2020**, *10*, 5336. [CrossRef]
39. Kingsley, K.; Barmawi, A. Improving Data Hiding Capacity in Code Based Steganography using Multiple Embedding. *J. Inf. Hiding Multimed. Signal Process.* **2020**, *11*, 14–43.
40. Budiman, G.; Suksmono, A.; Danudirdjo, D. *Compressive Sampling with Multiple Bits Spread Spectrum-Based Data Hiding*; 2020, in press.
41. Kao, D. Forensic Exchange Analysis of Contact Artifacts on Data Hiding Timestamps. *Appl. Sci.* **2020**, *10*, 4686. [CrossRef]
42. Khan, S.; Khan, M.N.; Iqbal, S.; Shah, S.Y.; Ahmad, N. Implementation of variable tone variable bits gray-scale image stegnography using discrete cosine transform. *J. Signal Inf. Process.* **2013**, *4*, 343–350. [CrossRef]
43. Khan, S.; Irfan, M.A.; Arif, A.; Rizvi, S.T.H.; Gul, A.; Naeem, M.; Ahmad, N. On Hiding Secret Information in Medium Frequency DCT Components Using Least Significant Bits Steganography. *Comput. Model. Eng. Sci.* **2019**, *118*, 529–546. [CrossRef]
44. Cintra, R.; Bayer, F. A DCT approximation for image compression. *IEEE Signal Process. Lett.* **2011**, *18*, 579–582. [CrossRef]
45. Wang, Z.; Bovik, A. A universal image quality index. *IEEE Signal Process. Lett.* **2002**, *9*, 81–84. [CrossRef]
46. Wang, Z.; Bovik, A.; Sheikh, H.; Simoncelli, E.P. Image quality assessment: From error visibility to structural similarity. *IEEE Trans. Image Process.* **2004**, *13*, 600–612. [CrossRef] [PubMed]
47. Boehm, B. Stegexpose—A tool for detecting LSB steganography. *arXiv* **2014**, arXiv:1410.6656.
48. Olson, E.; Carter, L.; Liu, Q. A Comparison Study Using StegExpose for Steganalysis. *Int. J. Knowl. Eng.* **2017**, *3*. [CrossRef]
49. Jia-Fa, M.; Xin-Xin, N.; Gang, X.; Wei-Guo, S.; Na-Na, Z. A steganalysis method in the DCT domain. *Multimed. Tools Appl.* **2016**, *75*, 5999–6019. [CrossRef]
50. Macq, B.; Dewey, F. Trusted headers for medical images. In *DFG VIII-D II Watermarking Workshop*; Elsevier: Erlangen, Germany, 1999; Volume 10, pp. 1–13.

51. Lin, Y.C.; Li, T.S. Reversible Image Data Hiding Using Quad-tree Segmentation and Histogram Shifting. *J. Multimed.* **2011**, *6*, 349–358. [CrossRef]
52. Jaiswal, S.P.; Au, O.; Jakhetiya, V.; Guo, A.Y.; Tiwari, A.K. Adaptive predictor structure based interpolation for reversible data hiding. In *International Workshop on Digital Watermarking*; Springer: Berlin, Germany, 2014; pp. 276–288.
53. Goljan, M.; Fridrich, J.; Du, R. Distortion-free data embedding for images. In *International Workshop on Information Hiding*; Springer: Berlin, Germany, 2001; pp. 27–41.
54. Vleeschouwer, C.; Delaigle, J.; Macq, B. Circular interpretation of histogram for reversible watermarking. In Proceedings of the 2001 IEEE Fourth Workshop on Multimedia Signal Processing, Cannes, France, 3–5 October 2001; pp. 345–350.
55. Khan, S.; Ahmad, N.; Ismail, M.; Minallah, N.; Khan, T. A secure true edge based 4 least significant bits steganography. In Proceedings of the 2015 International Conference on Emerging Technologies (ICET), Peshawar, Pakistan, 19–20 December 2015; pp. 1–4.
56. Alam, S.; Zakariya, S.M.; Akhtar, N. Analysis of modified triple A steganography technique using Fisher Yates algorithm. In Proceedings of the IEEE 14th International Conference on Hybrid Intelligent Systems (HIS), Kuwait, Kuwait, 14–16 December 2014; pp. 207–212.
57. Wang, C.M.; Wu, N.I.; Tsai, C.S.; Hwang, M.S. A high quality steganographic method with pixel-value differencing and modulus function. *J. Syst. Softw.* **2008**, *81*, 150–158. [CrossRef]
58. Khamrui, A.; Mandal, J. A genetic algorithm based steganography using discrete cosine transformation (GASDCT). *Procedia Technol.* **2013**, *10*, 105–111. [CrossRef]
59. Lee, C.; Chen, H. A novel data hiding scheme based on modulus function. *J. Syst. Softw.* **2010**, *83*, 832–843. [CrossRef]
60. Koikara, R.; Goswami, M. A Data Hiding Technique using Block-DCT. *Int. J. Eng. Res. Technol. IJERT* **2015**, *4*, 81–85.
61. Hou, D.; Wang, H.; Zhang, W.; Yu, N. Reversible data hiding in JPEG image based on DCT frequency and block selection. *Signal Process.* **2018**, *148*, 41–47. [CrossRef]
62. Wang, K.; Lu, Z.M.; Hu, Y.J. A high capacity lossless data hiding scheme for JPEG images. *J. Syst. Softw.* **2013**, *86*, 1965–1975. [CrossRef]
63. Huang, F.; Qu, X.; Kim, H.J.; Huang, J. Reversible data hiding in JPEG images. *IEEE Trans. Circuits Syst. Video Technol.* **2015**, *26*, 1610–1621. [CrossRef]