Journal of Theoretical and Applied Information Technology
15th January 2017. Vol.95. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A NOVEL SECRET IMAGE HIDING TECHNIQUE FOR SECURE TRANSMISSION

[1]S.MANIMURUGAN, [2]SAAD AL-MUTAIRI
[1]Assistant Prof., College of Computing and Informatics, Saudi Electronics University, Saudi Arabia
[2]Assistant. Prof., Computer Science and Information Technology Faculty, Tabuk University, Saudi Arabia.
E-mail: [1]smanimurugan@yahoo.co.in, [2]s.almutairi@ut.edu.sa

ABSTRACT

To transmit secret data from source to destination is a challenging task because there is a chance that intruders or third parties can hack the information at any moment. To address this problem, this paper proposed a new encryption technique called hybrid tailored visual cryptography and steganography (HTVCS) for secure transmission. In order to improve the algorithm complexity and strength, two popular methods were combined together in HTVCS. The original secret image was encrypted by modified tailored visual cryptography (MTVC). This MTVC encryption process can be classified into three processes: the pixel process, binary conversion and the share creation process. As a result, two encrypted shares were obtained. These shares were hidden inside a grayscale cover image in the steganography encode (SE) process using a key. The encoded image was sent to the receiver/authenticated person for the reconstruction process. In the decryption process, the encoded image was decoded by the steganography decode (SD) process using a key to obtain the share and cover images. In addition, the reconstructed shares were once again decrypted by MTVC decryption to retrieve the original secret image. The MTVC decryption can be divided into the following processes: re-swapping, share merging, decimal conversion and inverse pixel. The reconstructed secret image was validated by different parameters of the correlation coefficient (CC), the peak signal-to-noise ratio (PSNR), confidentiality, integrity and authentication (CIA) and complexity. As a result, the proposed HTVCS provided much better results than conventional methods. The main advantage of the proposed method is that a 98% exact replica of the secret image was retrieved and the algorithm complexity was improved due to the double encryption process. Therefore, it is very hard for intruders to hack the original secret data.
Keywords:
Keywords: *Modified Tailored Visual Cryptography, Steganography, Pixel Processing, Secret Key, Binary Conversion, Share Creation Process*

1. INTRODUCTION

Visual cryptography (VC) is a cryptography method where confidential or secret information is segregated into N number of shares for the secure transmission. On other hand, Steganography is an encryption scheme where secret information is hidden in a non-secret piece of data or in an image. The advantage of steganography is to prevent intruders or third parties from the hacking of secret information.

Based on the literature studies mentioned in section 2, VC and steganography are powerful encryption methods used to hide secret information for safe and secure transmission. However, to achieve the benefits of both methods, we proposed a novel hybrid tailored visual cryptography and steganography (HTVCS) scheme. This proposed method provides the characteristics of both TVC and steganography. Section three describes the TVC method and section four discusses the proposed HTVCS. The experimental results are discussed in section five. Acknowledgements and references are provided in sections six and seven, respectively.

2. LITERATURE SURVEY

To reconstruct the same original information, all N shares must be presented. If any share is not presented during the reconstruction process, it is very difficult to reconstruct the original image. To create the shares in the VC encryption process, two reference matrices plays a vital role. Many authors have proposed different VC techniques to encrypt secret images. However, in this section, we present different existing VC methods and analyse their

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

performance. Ching-Nung Yang et al. moved beyond conventional EVCS to CBW-EVCS . This method can be classified into construct CWB-EVCSs. All constructions were proven to satisfy security, contrast and cover image conditions [2, 10]. Roberto et al. proposed a visual cryptography scheme (VCS) to improve colour for black-and-white secret images [6, 8]. This proposed method is also called coloured-black-and-white VC. In the study's results, the colour was improved and pixel expansion was incorporated. To obtain the original pixels from the reconstruction process, the study provided general construction that allows the user to transform any black-and-white VCS. Finally, the authors had proven existing schemes comparison with optimal contrast differentiation for black-and-white pixels [11].

To transfer a secret medical image via a network, the authors proposed a novel VC scheme of tailored visual cryptography (TVC). In this scheme, the original secret medical image is encrypted and compressed. Due to these processes, the study's authors claimed that the original secret image was encrypted twice. The reconstructed image quality was good and it achieved higher CIA [3, 4, 7]. Another study presented a robust copyright protection scheme based on fractional FFT and VC [5, 9]. In this method, the author did not modify the original image; instead, the author used a visual secret sharing scheme (VSS). These shares were classified as master share and owner share. The owner share was created with the help of clandestine images obtained by VCS. The two shares generated did not give any information about the secret image. However, in order to be aware of the encrypted information, the created shares played a vital role. To achieve strength and security, the proposed scheme used the properties of FFT, SVD and VC.

Ahani et al. proposed a novel speech steganography method using discrete wavelet transform (DWT) and sparse decomposition (SD) to solve the identification problem in speech steganography. This proposed method of speech steganography exploits the additional representation of secret information within the next level of the non-secret image [1]. The authors proposed the use of the steganography method for hiding secret medical images in other medical images [12]. In this method an electroencephalogram (EEG) image was considered the secret image and a magnetic resonance image (MRI) was taken as the cover image. The patient information was encoded into a cover image. Fuzzy logic and non-sequential least significant bits (LSB) were chosen in this method. To prevent the attack, lossless compression and symmetric key encryption techniques were incorporated. The paper proposed a hybrid XOR coding and an edge detection-based steganography method for images. Integer wavelet transform (IWT) and spatial domain (SD) were used. The edge detection enables the credentials of sharp edges in a non-secret image that, when encoded, cause less degradation to the image quality compared to embedding in pre-specified pixels. It does not differentiate between smooth and sharp areas. The XOR is a simple, efficient technique that helps to minimise the differences between an encoded image and a non-secret image. The paper proposed a combination of the interpolation method and the compression technique for obtaining a high quality image [14]. This proposed interpolation method could provide a higher quality image. Audio steganography is also one method for encoding secret information into audio data. The paper notes that most of the proposed audio steganography techniques were not opted for real-time transactions/communication [15]. To overcome these issues, the authors invented a method called dual mode audio steganography (DMAS) based on FPGA . The implemented scheme processes obtained secret information at an encode rate of 25% with audio quality and the signal-to-noise ratio above 45 db. Another paper noted that the methods were orthogonal codes and steganography. The original biometric signatures were encoded by separate orthogonal codes and were multiplexed together [16]. After they were multiplexed, the images were embedded into a cover image via the steganography method. The cover image they had chosen for these processes was coloured. The multiple phase shifted reference joint transform correlation (MRJTC) was used for encryption and this technique was non-linear, which offered strong security against attacks.

3. TAILORED VISUAL CRYPTOGRAPHY SYSTEM (TVC)

This section discusses the TVC approach and its performance. The main advantage of this scheme is that the signal ratio of the reconstructed image was good and the entire process was completed without any post/preprocess. This technique was implemented for grayscale medical images. The proposed TVC was classified into two types of processes: TVC encryption and TVC decryption, as shown in Figure 1. In TVC encryption, the original secret image was converted

Journal of Theoretical and Applied Information Technology
15th January 2017. Vol.95. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

into a share image. The encrypted share image was decrypted by the TVC decryption (TVCD) process. Mostly, in the VC scheme, N number of shares will generate while encrypting the secret image. Instead, the proposed TVC provided one secret image, as shown in Equations 1, 2 and 3.

$$\Theta M_{(i,j)} = \Theta R_1 C_{1(i,j)} \oplus \Theta R_1 C_{2(i,j)} \oplus \Theta R_2 C_{1(i,j)} \oplus \Theta R_2 C_{2(i,j)} \quad (1)$$

$$\Theta M_{(i,j)} = \Theta R'_1 C'_{18bit(i,j)} \oplus \Theta R'_1 C'_{28bit(i,j)} \oplus \Theta R'_2 C'_{18bit(i,j)} \oplus \Theta R'_2 C'_{28bit(i,j)} \quad (2)$$

$$E_{12(i,j)} = \Theta R'_1 C'_{1Dec(i,j)} \oplus \Theta R'_1 C'_{2Dec(i,j)} \oplus \Theta R'_2 C'_{1Dec(i,j)} \oplus \Theta R'_2 C'_{2Dec(i,j)} \quad (3)$$

Creating a secret share involved five processes. The first process was the split process. In this process an original secret share was spilt into various sub-bands. The divided sub-bands' pixel values were converted into corresponding 8-bit binary values in the conversion process (Equation 2).

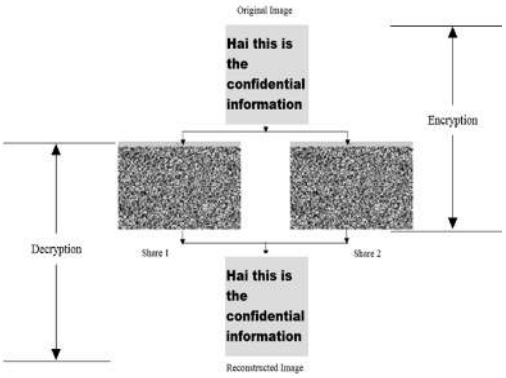


Figure 1: TVC Scheme for Secret Image.

The segregated N number of sub-bands was converted into 2N sub-bands in the pixel process. In this process, the image pixels were shuffled within the image itself. The shuffled 2N sub-bands were joined in different combinations. As a result, the 2N sub-bands were transformed into one sub-band in the merge process. This merged sub-band is also called a secret share. The literature review demonstrated that during reconstruction of the exact replica of a secret image, the pre/post process is a vital role in traditional VC schemes. Those problems occurred due to pixel expansion. But, in the TVCD process without any pre/post process, an exact replica of the secret image could be obtained [3, 4].

4. HYBRID TAILORED VISUAL CRYPTOGRAPHY AND STEGANOGRAP -HY (HTVCS) SCHEME

The TVC scheme and its performances were discussed in section three. This section describes the proposed HTVCS scheme. The main objective of this proposed system was to combine together TVC and steganography characteristics in one method. As a result, CIA can be improved to a greater extent than when using conventional methods. The proposed HTVCS can be classified into two divisions of encryption and decryption processes.

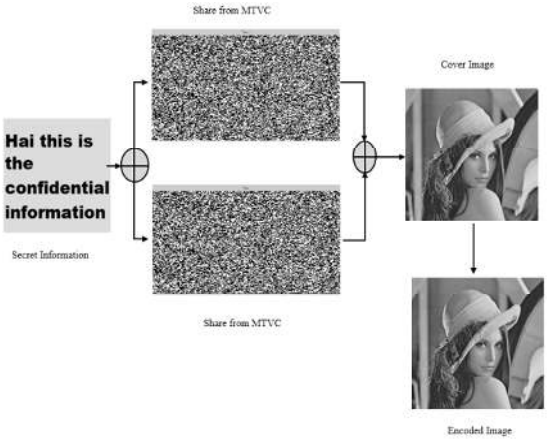


Figure 2: Hybrid Cryptography Encryption Process.

The TVC was proposed for the grayscale medical image transmission [3]. HTVCS encryption is segregated into two processes: modified tailored visual cryptography (MTVC) encryption and the steganography encode process. Likewise, decryption is also classified into MTVC decryption and the steganography decode process.

4.1. Modified TVC encryption process (MTVC) for secret image

The steganography method is used to hide a secret image within a cover/normal image. To achieve a higher CIA, the original secret image S_{ij} was converted into different shares in MTVC. The generated shares were encoded by the steganography method. Due to the processes mentioned above, double encryptions were

Journal of Theoretical and Applied Information Technology
15th January 2017. Vol.95. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

performed, thus making it difficult for intruders to hack secret image S_{ij}, as shown in Figure 3.

$$\sum S_{(i,j)} = \sum O_{c(i,j)} + \sum E_{c(i,j)} \quad (4)$$

$$\sum O_{c(i,j)} \oplus \sum E_{c(i,j)} = \sum S^1_{(i,j)} \quad (5)$$

$$\sum S_{(i,j)} = \sum O_{c(i,j)} + \sum E_{c(i,j)} = \sum O_{c(i,j)} \oplus \sum E_{c(i,j)} = \sum S^1_{(i,j)} \quad (6)$$

$$\sum S^1_{(i,j)} = \sum O_{r(i,j)} + \sum E_{c(i,j)} \quad (7)$$

$$\sum O_{r(i,j)} \oplus \sum E_{r(i,j)} = \sum S^2_{(i,j)} \quad (8)$$

$$\sum S^1_{(i,j)} = \sum O_{c(i,j)} + \sum E_{c(i,j)} \parallel \sum O_{r(i,j)} \oplus \sum E_{r(i,j)} = \sum S^2_{(i,j)} \quad (9)$$

$$\sum O_{r(i,j)} \oplus \sum E_{r(i,j)} \oplus \sum O_{c(i,j)} \oplus \sum E_{c(i,j)} = \sum S_{(i,j)} \quad (10)$$

$$\sum S^1_{(i,j)} \oplus \sum S^2_{(i,j)} = \sum S_{(i,j)} \quad (11)$$

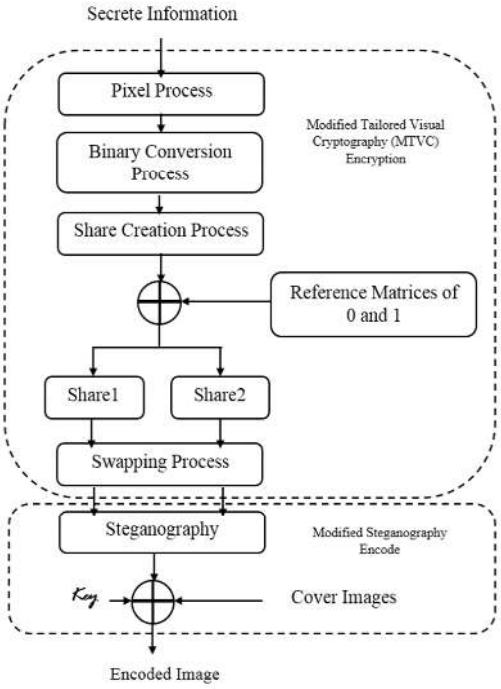


Figure 3 (a): Proposed Hybrid Cryptography Method: Encoding Process

In MTVC encryption, secret image S_{ij} was considered to be an input. The pixel process, the binary conversion process, the share creation process and the swapping process perform vital roles in MTVC encryption. In the pixel process, the S_{ij} was split into two different sub-bands of Oc_{ij} and Ec_{ij} in Equation 4. This separation was made based on the odd and even columns' pixels.

$$\sum S_{(i,j)} \Rightarrow \sum S^1_{(i,j)} \Rightarrow \sum S^2_{(i,j)} \quad (12)$$

$$\sum S^2_{(i,j)} \Longrightarrow Con_{(8bit)}\left[\sum S^2_{(i,j)}\right] \Longrightarrow \sum Bin_{(i,j)} \quad (13)$$

$$\sum Bin_{(i,j)} \oplus \prod_{i,j=0}^{m,n} R_{(i,j)} = \sum Sh^1_{(i,j)} + \sum Sh^2_{(i,j)} \quad (14)$$

This meant that the odd columns' pixels were in Oc_{ij} and the even columns' pixels were in Ec_{ij}. The separated sub-bands were combined together as an image S^1_{Ij} in Equations 5 and 6. In addition, the S^1_{Ij} was split into different sub-bands based on the odd row Or_{ij} and even row Er_{ij} pixels in Equation 7. The divided sub-bands were combined together as an image S^2_{ij} in Equations 8-12. The main advantage of the pixel process is that the pixel positions are interchanged as much as within the image itself. In the binary conversion process, every S^2_{ij} pixel was converted into corresponding 8-bit binary values Con_{8bit}. As a result, a binary image Bin_{ij} was obtained. The main reason is to use binary conversion that, to create a secret share image and this process is easier than other processes, as shown in Equation 13 and Figure 4.

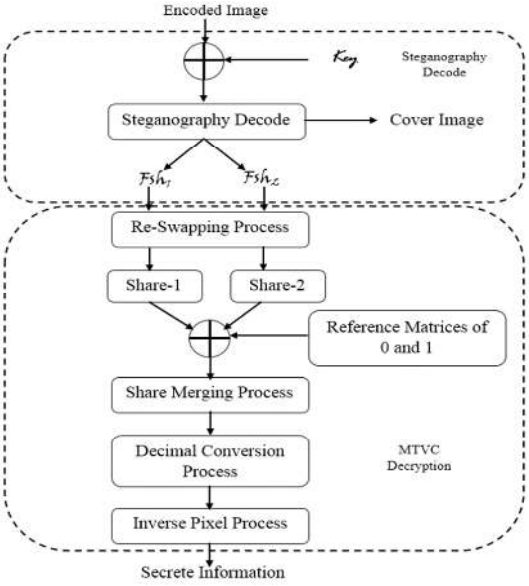


Figure 3(b): Proposed Hybrid Cryptography Method: Decoding Process.

After the binary conversion, the next process was the share creation process. In MTVC, the share

Journal of Theoretical and Applied Information Technology
15th January 2017. Vol.95. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

creation process plays an important role in creating the shares from Bin_{ij}. To create a binary image Bin_{ij}, the reference matrices Ref_{ij} are considered as an input, shown in Figure 5. From this process, two shares were created: Sh_{ij}^1 and Sh_{ij}^2. For example, consider a binary image and reference matrices as inputs. The binary pixels refer to the reference matrices that create the shares. If the pixel value is 1 or 0 it will find the corresponding matrix. As a result, one part of the reference pixels are placed in share1 and another part is placed in share2 (see Figure 6). The same steps are followed for the remaining pixels. Therefore, the binary image Bin_{ij} is segregated into two parts of share1 and share2.

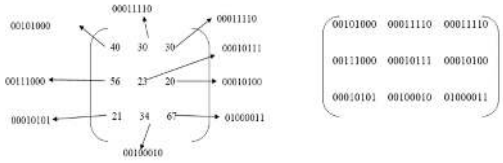


Figure 4: Binary Conversion Process

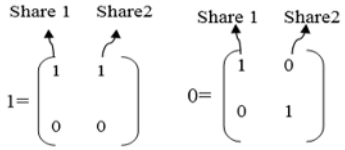


Figure 5:. Reference Matrices for 1 and 0.

Produced shares are once again taken for the swapping process. The aim of this process was to increase the complexity of the algorithm by swapping pixels as much as possible. The share1 was split, based on the odd columns OSh_{ij}^1 and even columns ESh_{ij}^1 separately in Equation 15.

$$\sum Sh_{(i,j)}^1 < \sum OSh_{(i,j)}^1 + \sum ESh_{(i,j)}^1 \quad (15)$$

$$\sum Sh_{(i,j)}^2 < \sum OSh_{(i,j)}^2 + \sum ESh_{(i,j)}^2 \quad (16)$$

$$\sum Bin_{(i,j)} \oplus \prod_{i,j=0}^{m,n} R_{(i,j)} = \sum OSh_{(i,j)}^1 + \sum ESh_{(i,j)}^1 + \sum OSh_{(i,j)}^2 + \sum ESh_{(i,j)}^2 \quad (17)$$

$$\sum OSh_{(i,j)}^1 \oplus \sum OSh_{(i,j)}^2 = \sum FSh_{1(i,j)} \quad (18)$$

$$\sum ESh_{(i,j)}^1 \oplus \sum ESh_{(i,j)}^2 = \sum FSh_{2(i,j)} \quad (19)$$

$$\sum FSh_{2(i,j)} + \sum FSh_{1(i,j)} = \sum Sh_{(i,j)}^1 + \sum Sh_{(i,j)}^2 \quad (20)$$

The same procedure was continued in share2 (Equations 16 and 17). The divided odd columns of share1 OSh_{ij}^1 and share2 OSh_{ij}^2 were combined. On the other hand, the even columns of share1 ESh_{ij}^1 and share2 ESh_{ij}^2 were also combined. Finally, two shares Fsh_1 and Fsh_2 were created from this process in Equations 18-20. However, in this proposed scheme, the pixel expansion was completed in order to improve algorithm strength.

4.2. Modified Steganography Encode Process for Shares

Steganography is one the foremost security techniques where confidential data/information can be embedded into an ordinary image so that the hidden secret information cannot be viewed by others. This means that hiding information in another image is a powerful method. This paper proposed a modified steganography method for hiding secret data. The grayscale image was considered as a cover image. The reason for choosing the grayscale image was that, during the encode time, if the last two bits values are changed, there is not much colour difference in the grayscale image. This is one of the main advantage for using this method to prevent data from being attacked.

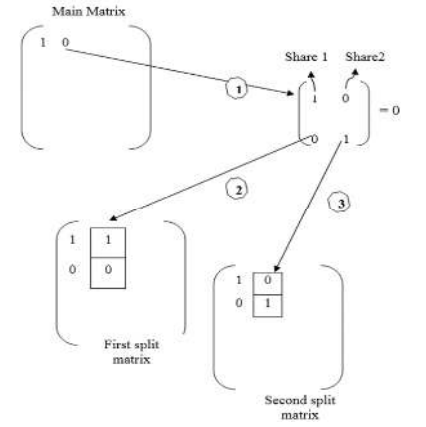
$$\sum C_{(i,j)} \Rightarrow Bin\left(\sum C_{(i,j)}\right) \Rightarrow \sum BC_{(i,j)} \quad (21)$$

$$Steg\left[\sum FSh_{1(i,j)}\right] = Key \oplus \sum_{i,j=0}^{m/2,n/2} BC_{lsb} \oplus \sum FSh_{1(i,j)} \quad (22)$$

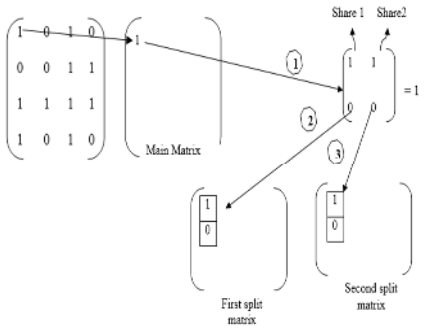
$$Steg\left[\sum FSh_{2(i,j)}\right] = Key \oplus \sum_{i=m/2,j=n/2}^{m,n} BC_{lsb} \oplus \sum FSh_{2(i,j)} \quad (23)$$

Journal of Theoretical and Applied Information Technology
15th January 2017. Vol.95. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195



(a)



(b)

Figure 6:. Share Creation Process with Example.

In this encode process, four pieces of input information were needed: the split shares Fsh_1 and Fsh_2 from the MTVC encryption, the grayscale cover C image and a key. The cover image pixels were converted into corresponding 8-bit binary in Equation 17. In every pixel in the cover image the LSB (the last two bits) were replaced by secret shares bits.

$$Steg\left[\sum FSh_{1(i,j)}\right] + Steg\left[\sum FSh_{2(i,j)}\right] = K\,ey \oplus \sum BC_{(i,j)} \oplus \sum S_{(i,j)} \quad (24)$$

$$Steg\left[\sum FSh_{1(i,j)}\right] + Steg\left[\sum FSh_{2(i,j)}\right] = \sum SI_{(i,j)} \quad (25)$$

$$\sum SI_{Dec(i,j)} \vDash \sum C_{(i,j)} \quad (26)$$

$$Key \rightarrow \sum BC_{lsb©2} \quad (27)$$

This meant that, in 8-bits of pixel, the last two bits were replaced by secret shares bits. The same process was continued up to the last pixel in Equations 24-26. The key shows how many LSB were concentrated in cover image $BC_{lsb©2}$ for the encode process in Equation 27. The obtained encoded image $SI_{(i,j)}$ was sent to the receiver/authenticated person to retrieve the confidential information.

4.3. Modified Steganography Decode Process

In this decode process, an encoded image $SI_{(i,j)}$ and key were considered for the reconstruction process. The encoded image's LSB were used for retrieving the hidden secret shares with the support of the key. The two secret shares and the cover image were reconstructed from this process in Equation 28. The retrieved swapped shares were Fsh_1 and Fsh_2, as shown in Figure 3b. After the decode process, the cover image and reconstructed cover image were not same due to the bit substitutions in Equation 29.

$$Steg_{Dec}\left[\sum SI_{(i,j)}\right] \oplus Key \Rightarrow \sum FSh_{1(i,j)} + \sum FSh_{2(i,j)} + \sum C'_{(i,j)} \quad (28)$$

$$\sum C'_{(i,j)} \neq \sum C_{(i,j)} \quad (29)$$

4.4. MTVC decryption process for retrieving the secret image

The steganography decode process provided three pieces of data: the cover image and the encoded shares Fsh_1 and Fsh_2. The yielded shares were considered to be an input in the MTVC decryption (MTVCD) process. The MTVCD process can be classified into re-swapping, share merge, decimal conversion and inverse pixel processes. In the re-swapping process, the input shares were split into two equal parts, as shown in Equations 30 and 31. The first share, Fsh_1, was divided into OSh^1_{ij} and OSh^2_{ij}. Similarly, Fsh_2 was segregated into ESh^1_{ij} and ESh^2_{ij}.

$$\sum FSh_{1(i,j)} \Rightarrow \sum OSh^1_{(i,j)} \oplus \sum OSh^2_{(i,j)} \quad (30)$$

$$\sum FSh_{2(i,j)} \Rightarrow \sum ESh^1_{(i,j)} \oplus \sum ESh^2_{(i,j)} \quad (31)$$

$$\sum OSh^1_{(i,j)} \bowtie \sum ESh^1_{(i,j)} \Rightarrow \sum Sh^1_{(i,j)} \quad (32)$$

$$\sum OSh^2_{(i,j)} \bowtie \sum ESh^2_{(i,j)} \Rightarrow \sum Sh^2_{(i,j)} \quad (33)$$

$$\sum Sh^1_{(i,j)} \bowtie \sum Sh^2_{(i,j)} \bowtie \prod_{i,j=0}^{m,n} R_{(i,j)} \Rightarrow \sum Bin_{(i,j)} \quad (34)$$

Journal of Theoretical and Applied Information Technology
15th January 2017. Vol.95. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$\sum Con_{B2D}\left[\sum Bin_{(i,j)}\right] \Rightarrow \sum S_{ij}^{2} \quad (35)$$

The separated shares were combined ⋈ based on odd and even columns. The reverse process of the swapping process can be called the re-swapping process, as shown in Equations 32 and 33. Two secret shares Sh_{ij}^{1} and Sh_{ij}^{2} were obtained from this process. The obtained shares were taken as an input for the share merge process. In this process, the binary image Bin_{ij} was generated by the given shares (Sh_{ij}^{1} and Sh_{ij}^{2}) and the reference matrices Ref_{ij}, as shown in Figure 5 and Equation 34.

$$\sum S_{(i,j)}^{2} \Rightarrow \sum S_{(i,j)}^{1} \Rightarrow \sum S_{(i,j)} \quad (36)$$

$$\sum S_{(i,j)}^{2} \Rightarrow \sum O_{r(i,j)} + \sum E_{r(i,j)} \quad (37)$$

For the binary image Bin_{ij}, every 8-bit was combined and converted into a corresponding decimal value S_{ij}^{2} in the decimal conversion process (Equation 35). This process was continued up until the last bit in Bin_{ij}. The obtained S_{ij}^{2} was considered to be an input for the inverse pixel process in Equations 36 and 37.

$$\sum O_{r(i,j)} \bowtie \sum E_{r(i,j)} = \sum S_{(i,j)}^{1} \quad (38)$$

$$\sum S_{(i,j)}^{1} \Rightarrow \sum O_{c(i,j)} + \sum E_{c(i,j)} \quad (39)$$

$$\sum O_{c(i,j)} \bowtie \sum E_{c(i,j)} = \sum S'_{(i,j)} \quad (40)$$

$$\sum S'_{(i,j)} = \sum S_{(i,j)} \quad (41)$$

In the inverse pixel process, the decimal image S_{ij}^{2} rows were split into two equal parts. The divided parts were merged as an image S_{ij}^{1} based on the odd and even row in Equation 38. Similarly, the S_{ij}^{1} was split into two equal parts based on the columns and the same process was applied to S_{ij}^{1} divided parts in Equations 39 and 40. After the merge process, the output was the original secret information $S'_{(i,j)}$ in Equation 41.

5. EXPERIMENT RESULTS AND DISCUSSION

In this section, the proposed scheme experiment results are presented. The 512x512 grayscale cover and the 128x128 secret images were considered to be inputs in this experiment. There were 1000 images taken for this study. In this paper, we have provided only four cover images and one secret image results. It is illustrated in Figures 7, 8 and 9.

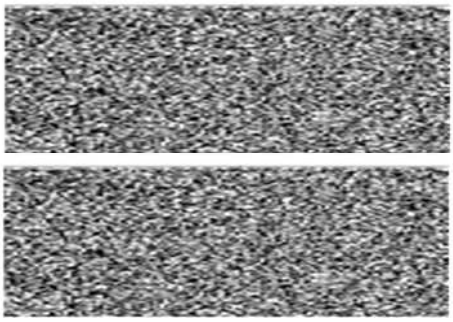


Figure 7: MTVC Encrypted Secret Image

Figure 8: Secret Image Before and After Process.

Table 1: Pixel Analysis

	Secret Information	*Total Number Of Pixels*	*Cover Image*	*Total Number Of Pixels*
Pixels	*128x128*	*16384*	*512x512*	*262144*
After Binary Conversion	*16384x8*	*131072*	*262144x8*	*2097152*
	Share creation process			
Share 1	*131072x2*	*262144*		
Share 2	*131072x2*	*262144*		
Total Required Pixels From Cover Image	*262144+ 262144*	*524288*	*2 Pixels Taken For Encode*	
			262144x (8-2)	*1572864*
		524288		***524288***

Journal of Theoretical and Applied Information Technology
15th January 2017. Vol.95. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

According to the pixel calculations, there are 16384 pixels in the 128x128 image. After the binary conversion, the total amount of bits was 131072, while there were 524288 bits after the share creation. During the steganography encode process the total number of cover image pixels was 262144; after the binary conversion, the total number of bits was 2097152. In the cover image every pixel's last two bits were replaced by secret bits in the encode process. As a result, from the 2097152 bits, 524288 bits' values were changed, as shown in Table 1.

To ensure the study achieved accurate results, we measured the algorithm performances using various parameters in our research laboratory. The considered parameters were CIA, CC, error rate, reconstructed image quality, encoded image quality and algorithm complexity and strength.

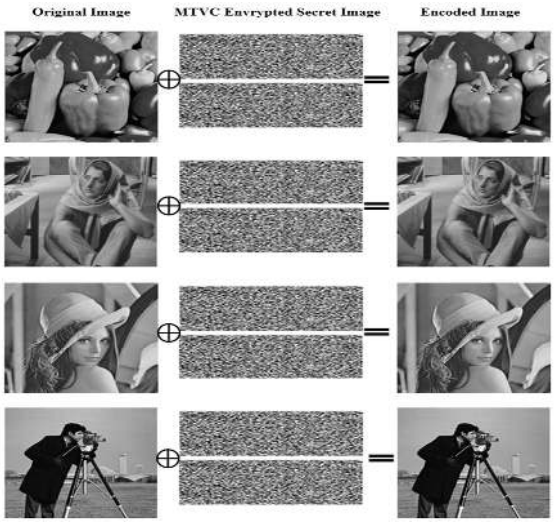


Figure 9: Grayscale Cover Image Before and After Process.

As we know, whenever security increases, it is clear that CIA is playing a key role. To ensure confidentiality, the secret image is converted into secret share and is also encoded into a cover image. The reconstructed secret image is validated in order to ensure integrity.

Table 2: Different Parameter-Based Analysis

Categories	*TVC*	*Steganography*	*Hybrid*
Integrity	*High*	*High*	*Too High*
Confidentiality	*High*	*High*	*Too High*
Authentication	*High*	*High*	*Too High*
Correlation Coefficient	*<1*	*<1*	*Near To Original*
Quality Of The Secret Information	*Good*	*Good*	*Good*
Error Rate	*Minimum*	*Minimum*	*Too Minimum*
Complexity	*High*	*Medium*	*Too High*
Strength	*High*	*Medium*	*Too Strong*

Due to the different processes, it is very hard for intruders to hack the secret image. Only the authenticated person can retrieve the secret image. In Table 2, the conventional steganography and VC methods are considered in comparison with the proposed scheme. Regarding CIA, the given conventional methods provided a good result. However, the proposed scheme achieved better results than the other methods due to the double encryption processes.

In the CC, we set the range from 0 to 1. When the CC value was close to 1, the proposed scheme obtained a near to original image; if it was set close to 0, it obtained an error message. The CC was calculated based on this point. As a result, compared with other conventional methods, the proposed scheme retrieved the exact replica of the original image and ensured integrity, as shown in Figures 10-14.

$$MSE = \frac{1}{m\,n}\sum_{i=o}^{m-1}\sum_{j=0}^{n-1}[O(i,j) - R(i,j)]^2 \quad (42)$$

$$PSNR = 10\ log_{10}(\frac{MAX^2}{MSE}) \quad (43)$$

To identify the image quality, the PSNR is one of the most common parameters used to measure the quality of reconstruction images in all areas. A higher PSNR generally indicates that the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

reconstruction image is of a higher quality but this may not occur in some cases. The PSNR is most easily defined via the mean squared error (MSE). From the monochrome m×n input image *O* and reconstructed image *R*, we could define the MSE in Equation 42 and the PSNR (in dB) in Equation 43.

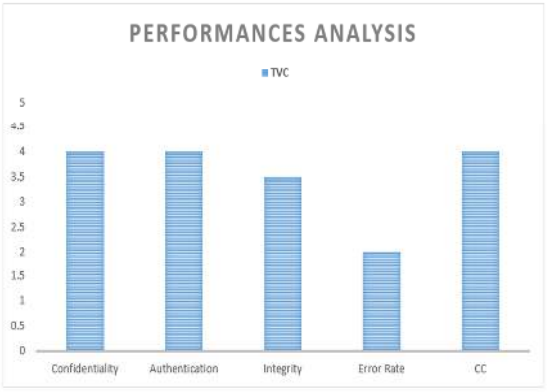


Figure 10: TVC Performance.

Figure 11: Hybrid Method Performance.

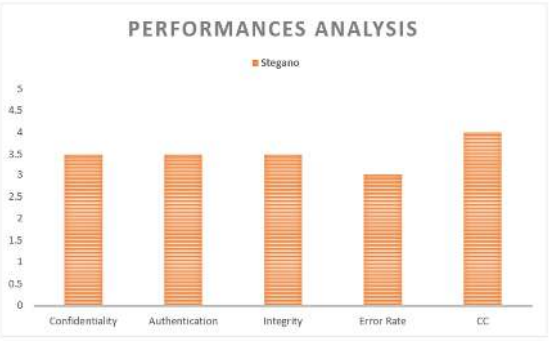


Figure 12: Steganography Performance.

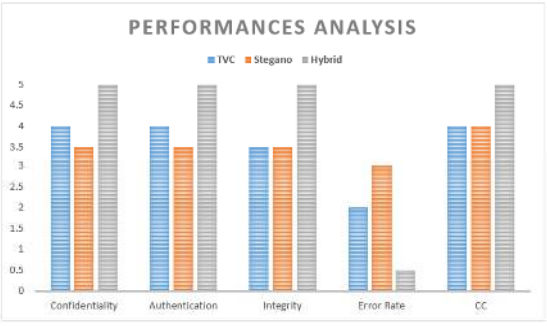


Figure 13: Comparison of Both Performance Analysis.

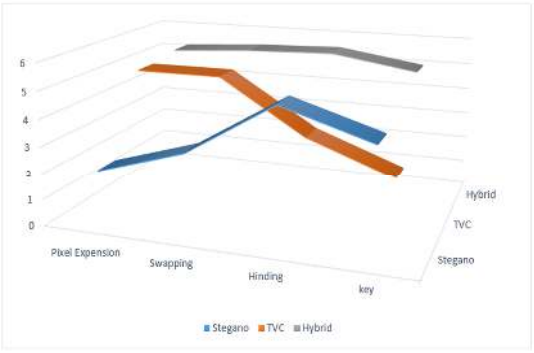


Figure 14: Comparison of Algorithm Complexity and Strength.

In terms of quality, comparing existing and proposed methods, the proposed method provided better quality than the other two methods due to the perfect design. Another important parameter is algorithm complexity.

To ensure complexity, the proposed scheme ensured that the pixels were interchanged as much as possible within the image itself and that pixel expansion was carried out (see Figure 14). Therefore, the proposed scheme provided better complexity and strength than the other methods. When comparing TVC and steganography, TVC provided better results than steganography, as illustrated in Table 2. The main aim of this proposed scheme was to achieve the features of TVC and steganography. From the results outlined above, our proposed method was superior to other methods.

6. CONCLUSION AND FUTURE WORK

Conventional TVC and steganography provided the best results in terms of complexity and strength. However, each method has its own merits that, pixel expansion, swipe the pixels as much as possible within the image, create secret shares, change the pixel values for hide a secret

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

information into cover image without affecting the visual quality and using a key. These are the main advantages of both methods. To combine the characteristics of both of methods we created the HTVCS scheme. The results have shown that this proposed method provided high confidentiality, integrity and authentication. To ensure confidentiality and authentication, the secret images were converted as shares and embedded inside a cover image. To ensure integrity, the reconstructed secret image was validated by the CC. In addition, the PSNR results were also superior when compared to conventional methods. We experimented with different attack processes, including pixel attack (PA) and human visual attack (HAV), in our research laboratory. The proposed algorithm performed well against both attacks. In the proposed encode process, the substitution of the bits and the procedure were entirely different from other substitution methods. Therefore, the proposed HTVCS method achieved high CIA, required less execution time for encryption and decryption, achieved a good PSNR and CC, achieved high complexity and good strength and retrieved the exact replica of the original secret image.

In the future, the same method with some modifications could be implemented in defense activities to transfer secret information from place to place.

7. ACKNOWLEDGEMENT

The authors would like to thank the Saudi Electronics University and Tabuk University, Saudi Arabia for giving immense support to carry out this research work. The suggestions and comments of anonymous reviewers for this accomplishment, which have greatly helped to improve the quality of this paper, are acknowledged. Special thanks to the editor for their support and valuable effort.

REFERENCES

[1]. Ahani, S., Iran, S., Ghaemmaghami, Z. and Wang, J. "A Sparse Representation-Based Wavelet Domain Speech Steganography Method", *IEEE Trans. on Audio, Speech, and Language Processing*, Vol.23, No.1, 2015, pp. 80-91.

[2]. Ching-Nung, Y., Li-Zhe, S. and Song-Ruei, C., "Extended Color Visual Cryptography for Black-and-White Secret Image", *Theoretical Computer Science*, Vol. 609, No.1, 2016, pp.143-161.

[3]. Manimurugan, S., and Narmatha, C.. "Secure and Efficient Medical Image Transmission by New Tailored Visual Cryptography Scheme with LS Compressions", *International Journal of Digital Crime and Forensics (IJDCF)*, Vol.7, No.1, 2015, pp.26-50.

[4]. Manimurugan, S., Porkumaran, K. and Narmatha, C., "The New Block Pixel Sort Algorithm for TVC Encrypted Medical Image", *Imaging Science Journal*, Vol.62, No.8, 2014, pp.403-414.

[5]. Rawat, S., and Raman, B., "A Blind Watermarking Algorithm Based on Fractional Fourier Transform and Visual Cryptography", *Signal Processing*, Vol.92, No.6, 2012, pp.1480-1491.

[6]. De Prisco, R. and De Santis, A., "Color Visual Cryptography Schemes for Black-and-White Secret Images", *Theoretical Computer Science*, Vol.510, 2013, pp. 62-86.

[7]. Stinson, D., "Visual Cryptography and Threshold Schemes", *IEEE Transaction on Potentials*, Vol.18, 1999, pp.13-16.

[8]. Tu, S. F. and Hou, Y. C., "Design of Visual Cryptographic Methods with Smooth-Looking Decoded Images of Invariant Size for Grey-Level Images", *The Imaging Science Journal*, Vol.55, 2007, pp. 90-101.

[9]. Zhongmin, W., Arce, G. R. and Di Crescenzo, G., "Halftone Visual Cryptography via Error Diffusion", *IEEE Transaction on Information Forensics and Security*, Vol.4, No.3, 2009, pp. 383-396.

[10]. Zhang, Xiaofei Wang, Wanhua Cao and Youpeng Huang., "Visual Cryptography for General Access Structure Using Pixel-Block Aware Encoding", *Journal of Computers*, Vol.3, 2008, pp. 68-75.

[11]. Yang, C. N., "New Visual Secret Sharing Schemes Using Probabilistic Method", *Pattern Recognition Letters*, Vol.25, 2004, pp. 481-494.

[12]. Karakis, R., Guler, I., Capraz, I. & Bilir, E., "A Novel Fuzzy Logic-Based Image Steganography Method to Ensure Medical Data Security", *Computers in Biology and Medicine*, Vol.67, No.1, 2015, pp.172-183.

[13]. Al Dmour, H. and Al Ani, A., "A Steganography Embedding Method Based on Edge Identification and XOR Coding", *Expert Systems with Applications*, Vol.46, 2016, pp.293-306.

[14]. Tang, M., Zeng, S., Xiaoliang Chen Jie Hu and Du, Y., "An Adaptive Image Steganography using AMBTC Compression and Interpolation Technique", *Optik International Journal for Light and Electron Optics*, Vol.127, No.1, 2016, pp. 471-477.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[15]. Haider Ismael Shahadi, Jidin, R. and Wong Hung Way. "Concurrent Hardware Architecture for Dual-Mode Audio Steganography Processor-Based FPGA", *Computers & Electrical Engineering*, Vol.49, 2016, pp.95-116.

[16]. M. Nazrul Islam, Muhammad Faysal Islam and Kamal Shahrabi., "Robust Information Security System Using Steganography, Orthogonal Code and Joint Transform Correlation", *Optik International Journal for Light and Electron Optics,* Vol.126, No.23, 2015, pp. 4026-4031.