A SECURE CIPHER FOR THE GRAY IMAGES BASED ON THE SHAMIR SECRET SHARING SCHEME WITH DISCRETE WAVELET HAAR TRANSFORM

Riyadh Jameel Toama¹, Nada Hussein M. Ali²

¹,²Department of Computer Science, University of Baghdad, Baghdad, Iraq

Corresponding Author: Riyadh Jameel Toama
Email: Riyadhjameel9@gmail.com

https://doi.org/10.26782/jmcms.2020.06.00025

Abstract

The rapid development in the technology of information and the necessity of transferring the information lead to the importance of the valuable and sensitive information protection is the major demand of users. Current research papers presenting a method for protection of a secret gray scale image and it is composed of four phases. First phase calculates the hash value using the SHA-256 type of hash function to make sure that there is no manipulating, altering or changing on the content of the secret image. The second phase is the encryption process for the secret image using the AES encryption algorithm. Third phase applied Shamir secret sharing scheme by splitting the encryption key of the encryption algorithm used in the previous phase into a number of shares. The final phase is for embedding secret image into an appropriate cover image using Discrete Wavelet Haar (DWH), the cover image is divided into four or more parts according to the iteration numbers that chooses manually. The Least Significant Bit (LSB) technique used for hiding the secret image in a cover image. The results obtained from the proposed method approved that the secret image completely restored without any change, moreover the correlation coefficient between the secret and the retrieved image is high. After the process of reconstruction of the stego image by the proposed method, the test results of quality of image were good with MSE 1.63 and PSNR 46.008 in Lena image.

Keywords: DWH, AES, LSB, MES, and PSNR.

I. Introduction

The growth of using the multimedia information increased the threats of losing that information in many ways, because of the sensitivity, privacy or secrecy of that information the demands on the protection of that information increased and be safe against any attacks that threaten that information. The protection of that information done in many methods and technique and most known technique and widely used the cryptography. Cryptography a technique or a method used for protection of valuable and secret information against any attacks from the
unauthorized people [XV]. The most know and widely used methods of cryptography are the encryption methods. The encryption method is a process of transforming the readable or recognizable data or information into unreadable or an unrecognizable form for the protection of that data or information while using or transferring from one side to another side, the encryption process done by many methods all methods categorized under two lines symmetric or asymmetric algorithms or methods [XI]. The symmetric algorithms or methods using one key for the encryption process and decryption process and also called one key algorithm, the asymmetric algorithms are using two keys one for encryption and the other one for decryption process. The most known algorithm is the advanced standard (AES) algorithm, AES is widely used because of it is the strongest encryption algorithm with a block size of 256-bit and 10, 12 or 14 rounds depending on the size of the key could be 64, 128 or 256-bit [XII]. The other concept of security is the secret sharing scheme. The secret sharing scheme is a method of splitting the secret information into a number of locations in order to increase the security of the secret information [VII]. The secret sharing scheme protects the secret information from the outside intruders or attackers; the strength of the secret sharing algorithm is the number of locations that the secret information sends the shares to it. The most known algorithm of secret sharing is the Shamir secret sharing scheme (ssss), the ssss is taking the secret information and process it after the processing it produces a number of shares. The shares are distributed among a number of participants; the requested number of shares to recover the secret information is the threshold of shares minus one [XIII]. The Discrete Wavelet Transform (DWT) has been used to separate the cover into a number of pieces in order to prepare that cover image for the process of hiding [XVIII].

II. Related Work

Numerous techniques and methods developed in the field of information security, such the cryptography, secret sharing, steganography and the DWT. Many researches concern the secret sharing scheme are listed in below:

In 2015, Kalist et al. [V] proposed a method of splitting an image that produced from the satellite by using a (DWT) because of the importance of that images, the segmentation of the satellite image is representing a challenge for the researchers who working on splitting the images. The proposed work taking the satellite images as RGB space, and convert it into the HSL space because the HSL space is the nearest to the human vision and also representing the accuracy much more than the RGB space.

In 2016, Shankar et al [VIII] proposed method of visual cryptography technique used the secret sharing with a high confidentiality and a simple and robust (k, n). In the process of sharing creation a new condition has been specified for the random matrices and performing the XOR operation for generating the n. The proposed method of (k, n) visual cryptography provides a strong protection for image while communicating.

In 2016, Liu et al [X] proposed a method of selecting a number of pixels (k) and a threshold for sharing (k,k) and extension threshold (k,n) to have a progressive
recovery with many shares and not losing any shares in recovery. The proposed method provides a simple computation for the process of dividing the original secret into shares also there no expansion of pixels and there is no alternative shadow image order in the process of recovery.

In 2016, Houssein et al [III] proposed a method of storing many messages in an image by using the steganography to make the capacity almost low, preserve the quality of the image, and maintain the confidentiality of the messages by using the cryptograph before storing it in the cover image. The proposed method gives a high security for the secret messages because of using the wavelet Haar method as a method of splitting the secret image into four sub bands and storing the secret in the lower band using the least significant bit LSB method.

In 2017, Gupta and Kaushik[I] proposed a method of reviewing two famous algorithms in cryptography the AES and RSA algorithms, the proposed work is intended to show the security of data over the communications of the channels by using symmetric and asymmetric algorithms. The data should be secured and not compromised and to achieve that the developers developing new policies against the attacks on that valuable information.

In 2018, Shankar et al [IX] proposed a method of encrypting shadow images using an encryption method called Homomorphic Encryption (HE) technique, the secret image has been exposed to the (DWT) and the result is producing asub-bands. Multiple shadows created and that shadows encrypted and decrypted for each of the shadows. The proposed method gives the highest levels of security because of secret key value is different with each image used that will add a high level of ambiguity to the method itself against any attack providing a very good security.

In 2018 Wenceslao et al [XVII] proposed a method of a multiple AES s-box the first one is replaced the Rijndael s-box in the cipher. The second created by performing an XOR operation and some transformation and replaced the mix column operation in the cipher. The experimental result shows that the performance of execution time increased by 27.5% in the encryption process and 108% in the decryption process with a minimum output bit change by 25%, the security still weak but the time of execution is greatly increased.

III. Advanced Encryption Standard (AES) Algorithm

The AES algorithm is one of the most famous and important algorithms in the field of communications in the security of information[I], is an algorithm used for the process of encryption and considered the most powerful algorithm, It is characterized by the key length and the block size that make it a strong algorithm for encryption. The main reason that the AES was created for was to fix the flaws and improve issues that found in the DES (Data Encryption Standard). The AES is a symmetric key algorithm, which means both users using the same encryption key. The standard encryption and decryption block size of data is 128 bits, and the size of the key is could be 128,192 or 256 bits using 10, 12 or 14 rounds based on key size.
IV. Shamir Secret Sharing Scheme (SSSS)

Shamir secret sharing is one of the secret sharing algorithms, where the secret divided into several parts among participants where the sum of the parts minus one needed for rebuilding the secret. Shamir secret sharing takes a number of \( k \) points to define polynomial of degree \( k-1 \). The basic idea of the creation of Shamir secret sharing was for the protection of cryptographic keys [II].

V. Hash Function

The hash function is a mathematical function type which transforming data to fingerprints of that data called hash. The hash function takes a random length message and gives an output with a fixed size acts as a message fingerprint [IV].

Fig.1: Represents SHA-256 Hash Function [IV]

VI. The Discrete Wavelet Haar (DWH)

The discrete wavelet Haar one of popular types of the discrete wavelet method used in digital images. The wavelet transform based on the principle of decomposition by breaking the discrete signal to multiple sub signals each has the half-length of the original and because of its simplicity; it could be taken as a reference for all types of transformations [XIII].

Dimension Wavelet Haar Transform

The 1-D (DWH) taking an input image and decompose it into four sub-bands, the splitting process is performed column by column and row by row respectively. The result is generating the four sub-bands called (LL, LH, HL, HH), the Low Low (LL) sub-band is the operational sub-band, it holds the whole operation that want to be applied to the image [XIV]. Figure 4 represents the aforementioned operation.
Fig. 2: Represents the 1-Dimension Discrete Wavelet Haar[VI]

Dimension Wavelet Haar Transform

The 2-D (DWH) taking an image as input and decomposes that image to four sub-bands, one represent the average component called Low Low (LL) and the other three represents the detailed components (LH, HL, HH). The 2-D (DWH) is used for edge detection of the original image, it can detect at each time three kinds of edges, and the other filters of edge detection cannot do that [XIV]. Figure 4 clarifies the aforementioned operation.

Fig. 3: Represents the 2-Dimension Discrete Wavelet Haar [VI]

VII. The Proposed System Structure

The proposed method is hiding a secret information represented as an encrypted secret image. Figure 4 demonstrates the main steps of the suggested system. The following phase describes each block in the Figure 4.
Fig. 4: Represents the Steps of the Proposed Work

Phase 1: Random Key Generation Algorithm:

The proposed key generation algorithm (KEY-GENR) creates the secret key in a random manner. The produced output key length will be 256-bit and it is used as input to the Shamir secret sharing algorithm. Algorithm 1 clarified the generation process.

Algorithm 1: Key generator Algorithm KEY-GENR

1. Input: Secret Key 256-bit, Register (X, Y, Z)
2. Output: Random Secret Key with 256-bit length
3. Start:
4. Step1: Assign a value to a variable called (Polynom).
5. Step2: Multiply the polynom * 16 to specify the no. of bits to the key will be generated (in the proposed method the key will be 256-bit so the polynom will be assigned to 16)
6. Step3: Divide the 256-bit over 8 times to specify the bytes numbers of bytes will be store in the register X.
7. Step4: take the result from the register and put it in a byte array and then use the random function to generate random numbers to the key

Copyright reserved © J. Mech. Cont.& Math. Sci.
Riyadh Jameel Toama et al
Phase 2: Encryption Process Using AES Algorithm

The secret image is encrypted using the Advanced Encryption Standard (AES) algorithm; the image after the process of encryption is the target that transfer from sender to receiver. The secret or encryption key that created by the proposed key generation algorithm (KEY-GENR) is the key use in this phase. The algorithm encrypts plain image in 128 bit block size with 256 bit key size. Algorithm 2 shows the encryption operation for the secret image.

Algorithm 2: AES Encryption Algorithm

1 Input: The Original image, Encryption Key 256 bits
2 Output: The Cipher image
3 Start;
4 Step1: Palin image (Original image).
5 Step2: Plain image XOR RoundKey (0)
6 Step3: For i = 1 to Nr (number of rounds).
7 If i != 0
8 SubBytes.
Phase 3: Shamir Secret Sharing Algorithm

The secret key that created by Algorithm 1 (KEY-GENR) will be used as input to the Shamir secret sharing algorithm. The Shamir secret sharing algorithm will produce a number of shares distributed to a number of participants. These shares will use later in the reconstruction of a secret key for the decryption process. Shamir (3, 4) threshold used for generating four shares of the secret encryption key. Algorithm 3 represents the main steps for splitting the secret key.

Algorithm 3: Shamir (3, 4) threshold secret sharing

1 Input: Secret Encryption Key (256-bit), n=4, k=3
2 Output: Four shares of key
3 Start:
4   Step1: For i = 1 to key length
5       Begin
6       Read key row (i)
7       Reading the random points from (key row(i), n)
8   Step2: For j = 1 to n
9       f(x) =
10       shares(x) = key length * 2
11       Produce the shares (x.share(x))
12   End for
Phase 4: Hash Function

The hash function taking a group of characters and maps those characters into a value with a certain length. In the proposed work, the SHA-256 is used which is a type of hash function that work as a one-way function. It converts any length of text into a string of 256 bits, using the SHA-256 in the proposed work gives that work cryptographically secure hashing function.

The encrypted image converted as a text file enter to the SHA-256 hash function, the resulted value represents as a signature to the cipher image. This process guarantees that any tamper to the encrypted image will completely yield another hash value. In this phase, the proposed system achieved two goals secrecy and integrity.

Fig. 5: Represents the Proposed Hash Function Work

Phase 5: The Discrete Wavelet Haar (DWH)

The discrete wavelet Haar a popular type of discrete wavelet method used in digital images. The wavelet transform has the ability to offer the information on the frequency domain and time domain concurrently, it is decomposes the image to four sub-bands the high frequency band (HH), the high low frequency band (HL), the low high frequency band (LH) and the low frequency band (LL). In (LL) the change between the pixels in small, the image is clear so the hiding of the secret performed in the (LL) sub band. The following is the execution algorithm (4) of DWHT:
Phase 6: The Proposed Hiding of Encrypted Image:

The encrypted image that is ciphered using the AES algorithm and the interrelated output value yield from the hash function will be hidden in a cover image; the steganography concealed method used is the Least Significant Bit (LSB) algorithm. The LSB method hiding the encrypted image values into the cover image pixels thought transforming the secret image into a matrix. After that, taking the index of each character that intended to be hidden in the cover image by transforming each character into an integer, consequently taking that value of the character and holds the index of a color element (R or G or B) that being processed currently. Algorithm 5 shows the main steps of this phase.
**Algorithm 5: Generating a position of cover image pixels by using (LSB)**

1. **Input:** Cover image, Encrypted image
2. **Output:** Cover Image with Hidden Secret Image Pixels Inside

3. **Start:**
   4. **Step1:** State matrix hiding $\leftrightarrow$ State matrix
   5. **Step2:** Holds the index
   6. $0 \leftrightarrow \text{charIndex}$
   7. value of the character that converted and the value of convert that character into integer
   8. $0 \leftrightarrow \text{charValue}$
   9. holds the color element (R or G or B) index that currently processed
   10. $0 \leftrightarrow \text{pixelElementIndex}$

11. **Step3:** For $i = 1$ to image height
   12. For $j = 1$ to image width
   13. Begin
   14. Getpixel $(j,i) \leftrightarrow \text{Pixel}$
   15. Clear each LSB from pixel element
   16. $R - R \% 2.$
   17. $G - G \% 2.$
   18. $B - B \% 2.$

19. **Step4:** For $k = 1$ to 3
   20. Begin
   21. Check if whole process has finished
   22. If $0 \leftrightarrow \text{Pixel index} \% 8$
   23. It is finish when 8 zeros added
VIII. PSNR and MSE Measures

Peak Signal to Noise Ratio called (PSNR) as an abbreviation and the Mean Square Error called (MSE) as an abbreviation are two kinds to measure the image distortion. PSNR is used to measure the image quality while the MSE is a mean square error for measuring among the cover image and the stage image [XVI]. The higher PSNR and the low MSE provide best results, and vice versa, they have defined:

\[
PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (1)
\]

\[
MSE = \left(\frac{1}{N}\right)^2 \sum_{i=1}^{N} \sum_{j=1}^{N} (x[i,j] - \bar{x}[i,j])^2 \quad (2)
\]

IX. Experimental Works and Results

This section presents the results that obtained from the proposed work. The system implemented using visual studio 2013, the C# programing language on a laptop with windows 7 operating system and CPU core 2 duo and 3GB of RAM. The evaluation factors are the Peak to Noise Ratio (PSNR) and Mean Square Error (MSE). The tests applied for evaluation of the performance of the proposed work, these tests are to measure the differences between the cover image quality, stego image quality and the image encryption quality. Figure 6 shows the difference in histogram between plain and encrypted Lena gray image of size 512*512. Table1 demonstrates some sample images of size 512*512 pixels and test another evaluation metric addition to PSNR and MSE to evaluate the proposed system.
Fig. 6: (a) Represent the original image (256*256) (b) represent the histogram of the original image (c) represent the encrypted image (d) represent the histogram of encrypted image

Gray Images Entropy

The entropy is measurement the original image and the ciphered image the result was that entropy is increased after encryption process, the increasing in the entropy vale means more distortion. The process of encryption is very good according to the results of the entropy. As illustrate in Table 1.

Table 1: Illustrate the Original Image and Entropy for Plain and Cipher Image and the Gray Correlation Coefficient between the Plain and Cipher Image

| Test Image | Entropy for Plain Image | Entropy for Cipher Image | Correlation Coefficient |
|------------|-------------------------|--------------------------|-------------------------|
| Lena       | 7.4451                  | 7.5554                   | -0.078                  |
| Airplane   | 6.7025                  | 7.5552                   | -0.0026                 |
| Bridge     | 5.7056                  | 7.5553                   | 0.048                   |

PSNR and MSE:

The result of the PSNR and MSE of the cover image and the secret image, the result illustrates the stego image is a high-quality image because the PSNR is high and the MSE is low so the produced stego image of the proposed system is very good in quality as illustrate in Table 2.
Table 2: Illustrations the Quality of Cover and Stego Image

| Test Image | Dimension Cover Image | Dimension Secret Image | MSE  | PSNR  |
|------------|-----------------------|------------------------|------|-------|
| Lena       | 512 x 512             | 256 x 256              | 1.63 | 46.008|
| Airplane   | 512 x 512             | 256 x 256              | 1.64 | 45.982|
| Bridge     | 512 x 512             | 256 x 256              | 1.66 | 45.929|

Fig. 7: (a) Represents Original Cover Image (512 X 512) (a1) Represents Histogram Of Cover Image, (a2) Represents Stego Image (512 X 512), (a3) Represents Histogram Of Stego Image

1- Dimension Wavelet Haar Transform:

The Table 3 denotes the required time needed for both transform and recovering operations.
Fig. 8: (b) Represents the 1-D (DWH) and (b1) represents the scheme for 1-D (DWH)

Table 3: The time elapsed to transform the cover image into 1-D in discrete wavelet Haar (DWH) measured in millisecond

| Cover Image | Dimensions | Time to Transform | Time to Recover |
|-------------|------------|------------------|-----------------|
| Barbara     | 512 x 512  | 1123 ms          | 1155 ms         |
| Lena        | 512 x 512  | 1014 ms          | 1092 ms         |
| Baboon      | 512 x 512  | 1202 ms          | 1039 ms         |

2-Dimension wavelet Haar transform:

The Table 4 indicates the necessary time for both transform and recover processes.

Fig. 9: (c) Represents The 2-Dimensional Discrete Wavelet Haar and (c1) Represents The Scheme for 2-D (DWH)
Table 4: The Time Elapsed to Transform the Cover Image into 2-D in Discrete Wavelet Haar (DWH) Measured in millisecond

| Cover Image | Dimensions | Time to Transform | Time to Recover |
|-------------|------------|-------------------|-----------------|
| Barbara     | 512 x 512  | 1202 ms           | 1263 ms         |
| Lena        | 512 x 512  | 1232 ms           | 1264 ms         |
| Baboon      | 512 x 512  | 1326 ms           | 1279 ms         |

X. Conclusion

The proposed method has three levels of protection. The first level of protection is the encryption of the secret image by using advanced encryption standard (AES) algorithm, the second level is the division for the secret key of the encryption process into a specific number of shares among a number of participants, and the secret key is generated randomly by a proposed method of key generation. The final level of protection is for hiding the encrypted image into cover image. The proposed work achieves the ability to detect any change in the secret encrypted image through using of hash function. The obtained results from the proposed method based on the standards that used to measure stego image quality after hiding the secret inside of it, also the quality of the secret image after decryption process, as well as the quality of an image that has been encrypted is good. The proposed method provides a very high level of security to secret image and the shares of a secret key for encryption that used for the secret image encryption.

References

I. Ashutosh Gupta, and Sheetal Kaushik. "A Review: RSA and AES Algorithm." IITM Journal of Management and IT, Vol.8, Issue 1, pp: 82-85, 2017.

II. Dahat, V. Ankush, and V. ChavanPallavi. "Secret sharing based visual cryptography scheme using CMY color space." Procedia Computer Science, Vol 78, Issue C, pp: 563-570, 2016.

III. Essam H. Houssein, Mona AS Ali, and Aboul Ella Hassanien. "An image steganography algorithm using haar discrete wavelet transform with advanced encryption system." 2016 Federated Conference on Computer Science and Information Systems (FedCSIS), pp:641-644, 2016.
IV. Je SenTeh, Kaijun Tan, and Moatsum Alawida. "A chaos-based keyed hash function based on fixed point representation." Cluster Computing, Vol. 22, Issue 2, pp: 649-660, 2019.

V. Jr. Wenceslao, V. Felicisimo "Enhancing the Performance of the Advanced Encryption Standard (AES) Algorithm Using Multiple Substitution Boxes." International Journal of Communication Networks and Information Security, Vol. 10, issue 3, p.496, 2018.

VI. Kaiser J. Giri, Mushtaq Ahmad Peer, and P. Nagabhushan. "A robust color image watermarking scheme using discrete wavelet transformation." IJ Image, Graphics and Signal Processing, Vol. 1, pp: 47-52, 2015.

VII. K. Shankar, and P. Eswaran. "Sharing a secret image with encapsulated shares in visual cryptography." Procedia Computer Science, Vol. 70, pp: 462-468, 2015

VIII. K. Shankar, and P. Eswaran. "A new k out of n secret image sharing scheme in visual cryptography." 2016 10th International Conference on Intelligent Systems and Control (ISCO), pp:1-6, 2016.

IX. K. Shankar, M. Elhoseny, R. S. Kumar, S. K. Lakshmanaprabu and X. Yuan, "Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique." Journal of Ambient Intelligence and Humanized Computing, pp: 1-13, 2018.

X. L. Liu, Y. Lu, X. Yan, and S. Wan, "A progressive threshold secret image sharing with meaningful shares for gray-scale image." 2016 12th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN), pp:380-385, 2016.

XI. M. Abdullah, "Advanced encryption standard (AES) algorithm to encrypt and decrypt data". Cryptography and Network Security, Vol. 16, 2017.

XII. M. M. Abdulwahid, O. A. S. Al-Ani, M. F. Mosleh and R. A. Abd-Almmeed. "Optimal access point location algorithm based real measurement for indoor communication". In Proceedings of the International Conference on Information and Communication Technology, pp: 49-55, 2019.

XIII. M. S. Sudha, and T. C. Thanuja. "Randomly tampered image detection and self-recovery for a text document using Shamir secret sharing." 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). IEEE, pp: 688-691, 2016.

XIV. Po-Cheng Wu, and Liang-Gee Chen. "An efficient architecture for two-dimensional discrete wavelet transform." IEEE Transactions on circuits and systems for video technology, Vol. 11, Issue 4, pp: 536-545, 2001.

Copyright reserved © J. Mech. Cont.& Math. Sci.
Riyadh Jameel Toama et al
R. Rahim, N. Kurniasih, F. Handayanna, L. S. Dewi, E. G. Sihombing, E. Arisawati, and I. Sulistiyowati. "Enhanced pixel value differencing with cryptography algorithm". In MATEC Web of Conferences, Vol. 197, p. 03011. EDP Sciences 2018.

Sahar A. El_Rahman, "A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information." Computers & Electrical Engineering, Vol. 70, pp: 380-399, 2018.

Thakral, Shaveta, and PratimaManhas. "Image Processing by Using Different Types of Discrete Wavelet Transform." International Conference on Advanced Informatics for Computing Research. Springer, Singapore, pp: 499-507, 2018.

V. Kalist, P. Ganesan, B. S. Sathish and J. M. M. Jenitha "Possiblistic-Fuzzy C-means clustering approach for the segmentation of satellite images in HSL color space". Procedia Computer Science, Vol. 57, pp: 49-56, 2015.