Journal of Theoretical and Applied Information Technology
15th May 2018. Vol.96. No 09

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

# A HYBRID TEXT – IMAGE SECURITY TECHNIQUE

**[1]SALEH SARAIREH, [2]JAAFER AL-SARAIREH, [3]YAZEED AL-SBOU, [4]MOHAMMAD SARAIREH**

[1]Al-Hussien Bin Talal University, Jordan
[2]Princess Sumaya University for Technology, Jordan
[3]Mutah University, Jordan
[4]Mutah University, Jordan
E-mail: [1]saleh_53@yahoo.com, [2]j.saraireh@psut.edu.jo, [3]yazeed1974@gmail.com, [4]m_srayreh@mutah.edu.j

**ABSTRACT**

The transmission of a secret message or secret image over public networks may be affected by several types of security attacks. This problem triggered the researcher to implement secure algorithms that provide the security services, and at the same time to protect the transmitted data through the communication channel.

There are many applications that involve the transmission of secret text messages and secret image, such as, medical images with radiologist reports, exam, questions that involve text and images and government applications that require images and text. This paper comes to address the security of such applications, so a security technique is proposed. It involves the embedding of secret text message over a secret image using wavelet and genetic algorithm based steganography, and then the generated stego image is encrypted using a filter bank cryptographic algorithm, also hashing algorithm is used to ensure data integrity.

Security performance metrics are used to assess the proposed technique; this involves normalized correlation, PSNR, histogram analysis, and entropy. Based on the proposed algorithm, the obtained results showed that a high level of security has been achieved.

**Keywords:** *Image Encryption, Hashing, Steganography, Entropy, Correlation*

## 1. INTRODUCTION

Due to the vast advances and developments in the Internet and communication networks types and techniques, information security requirements are increased and became almost complicated. Consequently, the security of information transmitted through these networks, especially the public ones, may sever of a big chance for a third party to access this information [1]–[3]. Therefore, users need their information to be hidden and transferred safely, securely and with high confidentiality due to the insecure pathways which may be utilized for sharing files or information. Based on this, information must be hidden and highly protected by converting it into cryptic format [4][5]. Several techniques were proposed to ensure information security hiding and confidentiality during transmission. These methods are like steganography and cryptography.

Cryptography is the art and science of keeping messages secure by converting them from one form to another. Several cryptography algorithms such as Advanced Encryption Standard (AES), DES, and International Data Encryption Algorithm (IDEA) [6] were implemented for data encryption. These algorithms are suitable for encryption of least amount of data however they are not suitable when the data to be encrypted is huge. That is because these algorithms need large computation times and therefore super-fast processing machines. Alternatively, steganography is based on data embedding or hiding. This is based on embedding data into other multimedia applications like video, image or audio in a way that no one can infer or extract the embedded data.

Therefore, steganography hides a text so it is hard to be noticed whereas cryptography scrambles the text so it is hard to be recognized [7]. Hence, each approach provides information security; therefore, combining both of them in one system enhances the information confidentiality and security [8]–[10].

The image is the most commonly used as a cover medium for steganography. Steganography algorithms are categorized into two types: spatial

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

and frequency domains [11]. The spatial domain one's employ pixel gray level for encoding the message bits like the Least Significant Bit (LSB) algorithm. While message bits are encoded in the transform domain coefficient of the image in the frequency domain methods like the Discrete Fourier Transformation (DFT), Discrete Cosine Transformation (DCT), and Discrete Wavelet Transformation (DWT).

This paper is structured as follows. Previous research studies and literature are presented in section 2. In section 3, the implementation of the proposed techniques is presented. The security analysis and discussion are introduced in section 4. Final, Section 5 concludes our work.

## 2. RELATED WORK

Several image steganography algorithms were proposed in the literature. Example of these algorithms is discussed in the followings. LSB, which is one of the most common image steganography algorithms used to insert secret data in images. The LSBs of the cover image is changed so that secret message or text can be embedded within it [12].

As mentioned above, to improve security, cryptography is combined with steganography. In addition, compression algorithms may be included in order to increase the payload capacity of the stego-object. Example of this was proposed in [12], [13] where the Lempel-Ziv-Welch (LZW) lossless compression technique [14] was applied in order to reduce the hidden text size before encryption. Then, the Tiny Encryption Algorithm (TEA) combined with the LSB method was used to conceal messages inside the cover image.

In [15], colored images were encrypted by the lossless symmetric image cryptography using the substitution/diffusion structure. The results of this approach showed the possibility of managing the tradeoffs between the security and speed which made it appropriate for secure real-time image and video transmissions.

In [16], a steganography approach was proposed where the message is encrypted by DES [17]. Then, the encrypted message data is embedded into the cover image by using the LSB technique. DES was commonly used because it is a symmetric algorithm and more secure when there is a use of a hash key.

In [18] an improved LSB technique was used. In this paper, before data embedding into the image, it was encrypted by the SDES algorithm. Then, images were classified into smooth areas and edges. The LSB technique is performed in the edge areas only. The AES cryptography with the aid of the LSB image steganography was used for hiding the sensitive data on the given cover image [19]. This approach, firstly compressed the data to be embedded, then employs the AES algorithm to produce the cipher text which is broken into small blocks to be embedded into the image. The image is processed by a genetic algorithm to choose the rows and low-intensity pixels to hide data on the LSB of the image.

Usually, hashing algorithms are employed to satisfy the data integrity. These algorithms are like Message Digest 5 (MD5) [20] Secure Hash Algorithm (SHA) [21]. Both MD5 and SHA have some limitations in terms of vulnerability, slow and unsuitable for a large amount of data. In [22], a novel hash-based steganography algorithm for hiding and extracting of embedded data in grayscale images was proposed. This algorithm inserts a group of bits in one block while other algorithms embed only one or two bits. A novel hash-based steganography method for the colored image was proposed in [23]. In order to overcome the drawbacks of colored image steganography approaches in terms of massive data, vulnerability, and speed, which apply chaos and symmetric-key cryptographic methods, this method employed a perfect hash function approach to sustain a secure and fast mechanism suitable for steganography of colored image.

In [24], to afford more security, a new approach based on using the Hash LSB combined with an affine cipher mechanism was employed. This was used to encrypt the message to be hidden it inside a colored image. Then, the encrypted message bits were inserted in the pixels of the colored image based on applying a hash function to choose the specific location in LSBs.

All previous literature concentrated on the confidentiality service for a secret text or a secret image separately, moreover, the data integrity service is not considered. Some applications require the transmission of secret text and secret image at the same time, how the confidentiality and data integrity can be satisfied. Nevertheless, the significance of the combination of both steganography and cryptography in encrypting and securing information transmission, but still there is always a continuous need for new enhanced algorithms to be more efficient and secure. This may be accomplished by adding another stage which improves the existing algorithms. This stage

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

is represented by utilizing a hashing function which will add integrity service for these algorithms as introduces in this paper.

## 3. THE PROPOSED TECHNIQUE

The main processes in the proposed technique are hashing, steganography, and image encryption. Confidentiality is satisfied by employing a strong steganography and image encryption algorithms. On the other hand, data integrity is satisfied by using a hashing function. The operational steps are depicted in Figure (1), 2 and 3. These operational steps involve:

- **At the sender:**

  a- Hashing the secret message by using a secure hash algorithm 3 (SHA3), to generate a hash value. SHA – 3 – 256 generates a hash value of 256 bits' length for variable input.

  b- Encapsulating the generated hash value with the secret message to generate a concatenated data

  c- Hiding the concatenated data into a cover image to produce the stego image, where this image is a secret image. The hiding process is achieved using a combination of the wavelet transform and genetic algorithm. This steganographic algorithm is employed in this research, since it provides a high hiding capacity [25].

  d- Encryption of the stego image to generate an encrypted image. This operation involves the encryption of the secret image and the hidden secret data simultaneously, since the secret data is hided inside the secret image. So, instead of encrypting the secret message separately and then encrypt the secret image, only one encryption process is done. The filter bank symmetric cryptography technique is employed in order to perform image encrypting using a particular key [26].

  e- Sending of the encrypted image to the destination over a non–secure communication channel.

- **At the receiver:**

  a- Decryption of the received encrypted image to generate the corresponding stego image. The same secret key used for encryption process is used to execute the decryption process. Since the symmetric cryptographic algorithm is employed.

  b- The Extracting process is used to obtain the secret image and the concatenated data.

  c- Splitting the concatenated data to a secret data (message) and a hash value.

  d- To verify data integrity, the hash value for the obtained secret data is computed and compared with the received hash value. If the same hash value is generated, then the integrity service is satisfied properly, otherwise, the verification process is failed.

| **Algorithm 1:** Encoding Secret Data and Image |
|---|
| **Input:** Secret Data, Secret Key, Secret Image<br>**Output:** Encrypted Image |
| Hash Value = SHA-3-256(Secret Data)<br>Result = Append (Hash Value, Secret Data)<br>Stego Image = Embedding (Result, Secret Image)<br>Encrypted Image = Encryption (Stego Image, Secret Key) |

*Figure 2: Algorithm of Encoding of Secret Data and Image*

| **Algorithm 2:** Extraction of Secret Data and Image |
|---|
| **Input:** Encrypted Image, Secret Key<br>**Output:** Secret Data, Secret Image |
| Stego Image = Decryption (Encrypted Image, Secret Key)<br>Secret Image, Concatenated Data = Extracting (Stego Image)<br>Hash Value Secret Data = Extract (concatenated Data)<br>Compute Expected Hash Value = SHA-3-256(Secret Data)<br>If (Expected Hash Value = Hash Value)<br>Successful Verification<br>Else<br>Fail Verification |

*Figure 3: Algorithm of Extraction of Secret Data and Image from Encrypted Image*

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

## 4. SIMULATION RESULTS & SECURITY ANALYSIS

Two secret images are used in this research to study the security performance of the proposed method. The security performance is investigated by using many metrics. The size of each image is 256×256 pixels with a depth of 8 bits.

The security of the proposed technique is examined by comparing the original stego image with the encrypted one; the images must be highly uncorrelated to ensure high-security level. Several metrics can be used to measure the correlation, namely, normalized correlation, PSNR, histogram analysis, and entropy.

Normalized correlation is a key metric that can be used to measure the similarity between two images. If the correlation factor between the two images: the original and the encrypted one is very low or very close to zero, then, the images are completely different and the encryption process is strong, but if the correlation factor is equal to one, the images are identical and the encryption process is very weak. In this research, two benchmark images, namely the MRI and WOMAN were used. The correlation factor is measured for these two images and the corresponding encrypted images. As summarized in table (1), the correlation factors are very low. This indicates that the proposed technique can conceal all features of the transmitted image; consequently, the required security is satisfied.

The similarity between the encrypted image and the original one is evaluated by the PSNR. PSNR is calculated for MRI and WOMAN images and their encrypted images. PSNR values are summarized in Table (1). It is clear that these values are very low which proves that the images are uncorrelated, and thus high security is realized.

*Table 1: Security Analysis Results.*

| Image | Corr. Factor | PSNR (dB) | Entropy |
|---|---|---|---|
| MRI | 0.0042 | 11.2451 | 7.9875 |
| Women | 0.0026 | 10.7631 | 7.9945 |

Moreover, the randomness and uncertainty of the encrypted image is measured using the Entropy Usually, for the truly random grayscale image, the entropy is 8 bits/pixel. So, as the entropy gets closer to 8 bits/pixel of the encrypted image, accordingly, the degree of randomness and confidentiality is higher. To calculate the entropy, MRI and WOMAN images are encrypted using the proposed technique. As illustrated in Table (1), the entropy values are much closer to the theoretical value; this indicates that the encryption operation generates a random image.

To study the statistical similarity and the visual correlation between the original and the encrypted images, image histogram analysis is employed. This histogram gives the distribution of each gray level. Histograms of both images are shown in Figure 4 and Figure 5. Note that, there is a large difference between the histogram of the encrypted and the original ones; this means that, both are highly uncorrelated. Also, the histograms of the encrypted images indicate that the gray levels are uniformly and equally distributed. So, for the used images, it can be noticed that there is no visual correlation or similarity before and after encrypting process, which means that the confidentiality is achieved.

The proposed technique is compared with three of the existing techniques. The proposed technique provides confidentiality and integrity for the secure data, while the other techniques provide only confidentiality. This limitation makes the proposed technique superior to other techniques. So, the major contribution of the proposed technique is the satisfaction of confidentiality and integrity. This comparison is presented in Table 2.

*Table 2: Comparing achievements of confidentiality and Data integrity*

| Algorithm | Confidentiality | Data Integrity |
|---|---|---|
| Proposed Technique | Yes | Yes |
| [9] | Yes | No |
| [15] | Yes | No |
| [23] | Yes | No |

## 5. CONCLUSION

Mutual security technique is proposed in this research. It combines image encryption, hashing algorithm, and wavelet transform and genetic algorithm based steganography. This combination improves the confidentiality and data integrity.

This research focuses on the applications that involve the sending of the secret image and secret text message at the same time. To achieve the confidentiality, the secret message is hidden into the

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

secret image using wavelet transform and genetic algorithm based steganography, and then the secret image is encrypted using filter bank block cipher. To achieve data integrity, SHA – 3 – 256 hash function is employed to produce a hash value of the secret message at the transmitter side and receiver side.

The simulation results obtained in terms of normalized correlation, PSNR, entropy, and histogram analysis are very close to theoretical values. As a result, the proposed technique is secure and efficient.

One more direction of this research is to satisfy all the security services (confidentiality, data integrity, and authentication), since the authentication service does not satisfy in this research.

**REFERENCES:**

[1] M. S. Sreekutty and P. S. Baiju, "Security enhancement in image steganography for medical integrity verification system," in *2017 International Conference on Circuit ,Power and Computing Technologies (ICCPCT)*, 2017, pp. 1–5.

[2] J. Al-Saraireh, "An efficient approach for query processing over encrypted database," *J. Comput. Sci.*, vol. 13, no. 10, pp. 548–557, 2017.

[3] J. Al-Saraireh, "HVM: A method for improving the performance of executing SQL-query over encrypted database," *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 14, pp. 3394–3402, 2017.

[4] P. R and Iswarya R.J, "An Overview of Digital Image Steganography," *Int. J. Comput. Sci. Eng. Surv.*, vol. 4, no. 1, pp. 23–31, 2013.

[5] M. H. Abood, "An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms," in *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*, 2017, pp. 86–90.

[6] K. Usman *et al.*, "Medical Image Encryption Based on Pixel Arrangement and Random Permutation for Transmission Security," in *2007 9th International Conference on e-Health Networking, Application and Services*, 2007, pp. 244–247.

[7] R. Singh Chhillar, "Data Hiding using Advanced LSB with RSA Algorithm," *Int. J. Comput. Appl.*, vol. 122, no. 4, pp. 975–8887, 2015.

[8] A. J. Raphael and V. Sundaram, "Cryptography and Steganography – A Survey," *Int. J. Comput. Technol. Appl.*, vol. 2, no. 3, pp. 626–630, 2011.

[9] S. S. Saraireh, M. S. Saraireh, S. S. Saraireh, and M. S. Saraireh, "Filter Bank Block Cipher and LSB Based Steganography for Secure Data Exchange," *Int. J. Commun. Antenna Propag.*, vol. 7, no. 1, p. 1, Feb. 2017.

[10] S. Saraireh, "A Secure Data Communication System Using Cryptography and Steganography," *Int. J. Comput. Networks Commun.*, vol. 5, no. 3, 2013.

[11] S. M. Mohidul Islam, A. Hossin, R. K. Shah, and P. K. Bipin, "Bit Adjusting Image Steganography in Blue Channel using AES and Secured Hash Function," *Int. J. Comput. Sci. Mob. Comput.*, vol. 611, no. 11, pp. 25–30, 2017.

[12] Y.-K. Lee, G. Bell, S.-Y. Huang, R.-Z. Wang, and S.-J. Shyu, "An Advanced Least-Significant-Bit Embedding Scheme for Steganographic Encoding," Springer, Berlin, Heidelberg, 2009, pp. 349–360.

[13] A. D. Ker, "Steganalysis of LSB matching in grayscale images," *IEEE Signal Process. Lett.*, vol. 12, no. 6, pp. 441–444, Jun. 2005.

[14] W. Kinsner and R. H. Greenfield, "The Lempel-Ziv-Welch (LZW) data compression algorithm for packet radio," in *[Proceedings] WESCANEX '91*, pp. 225–229.

[15] V. Patidar, N. K. Pareek, and K. K. Sud, "A new substitution–diffusion based image cipher using chaotic standard and logistic maps," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 14, no. 7, pp. 3056–3075, Jul. 2009.

[16] V. LokeswaraReddy, A. Subramanyam, and P. Chenna Reddy, "A Novel Approach for Hiding Encrypted Data in Image, Audio and Video using Steganography," *Int. J. Comput. Appl.*, vol. 69, no. 15, pp. 37–44, May 2013.

[17] T. Nie, C. Song, and X. Zhi, "Performance Evaluation of DES and Blowfish Algorithms," in *2010 International*

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

*Conference on Biomedical Engineering and Computer Science*, 2010, pp. 1–4.

[18] M. Juneja and P. S. Sandhu, "An Improved LSB Based Steganography Technique for RGB Color Images," *Int. J. Comput. Commun. Eng.*, vol. 2, no. 4, pp. 513–517, 2013.

[19] P. Sethi and V. Kapoor, "A Secured System for Information Hiding in Image Steganography using Genetic Algorithm and Cryptography," *Int. J. Comput. Appl.*, vol. 144, no. 9, pp. 975–8887, 2016.

[20] Z. Yong-Xia and Z. Ge, "MD5 Research," in *2010 Second International Conference on Multimedia and Information Technology*, 2010, pp. 271–273.

[21] N. Abdoun, S. El Assad, M. A. Taha, R. Assaf, O. Deforges, and M. Khalil, "Secure Hash Algorithm based on Efficient Chaotic Neural Network," in *2016 International Conference on Communications (COMM)*, 2016, pp. 405–410.

[22] G. J. Chhajed and S. A. Shinde, "Efficient embedding in B&W picture images," in *2010 2nd IEEE International Conference on Information Management and Engineering*, 2010, pp. 525–528.

[23] R. Riasat, I. S. Bajwa, and M. Z. Ali, "A hash-based approach for colour image steganography," in *International Conference on Computer Networks and Information Technology*, 2011, pp. 303–307.

[24] A. M. Abdullah, R. Hikmat, and H. Aziz, "New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm," *Int. J. Comput. Appl.*, vol. 143, no. 4, pp. 975–8887, 2016.

[25] G. Elham, S. Jamshid, and Nima Fassihi, "High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm," in *International MultiConference of Engineers and Computer Scientists* , 2011, pp. 495–498.

[26] S. Saraireh and M. Benaissa, "A Scalable Block Cipher Design Using Filter Banks and Lifting over Finite Fields," in *2010 IEEE International Conference Acoustics Speech and Signal Processing (ICASSP)*, Dallas, TX, USA.

Journal of Theoretical and Applied Information Technology
15th May 2018. Vol.96. No 09

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

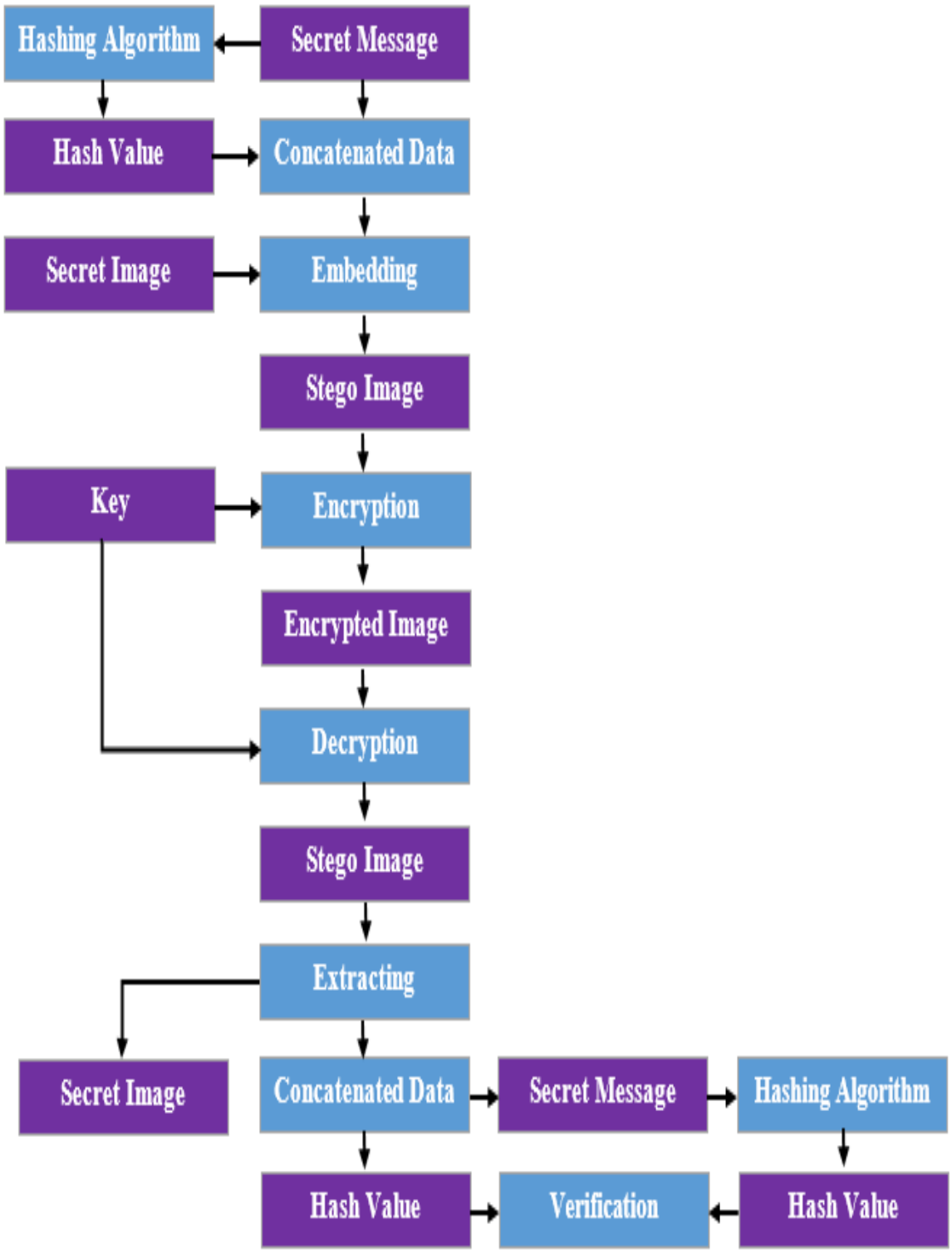
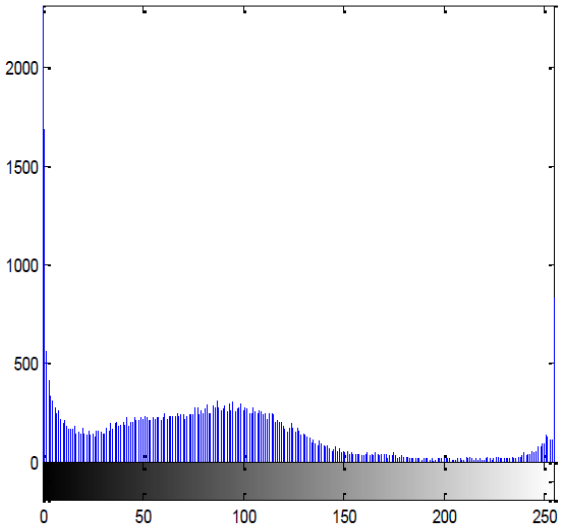


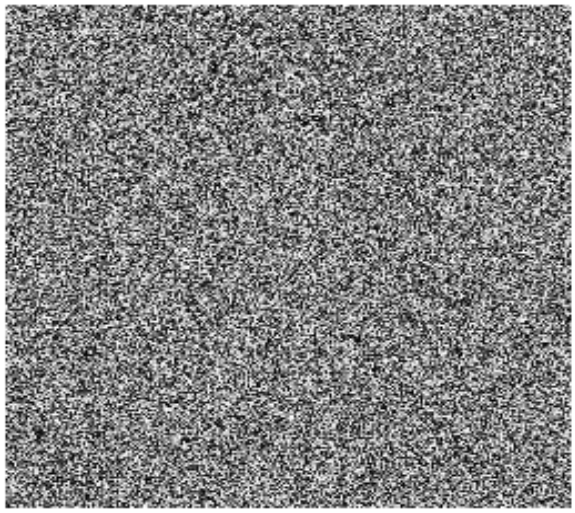

*Figure 1: Block Diagram of the Proposed Algorithm*

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

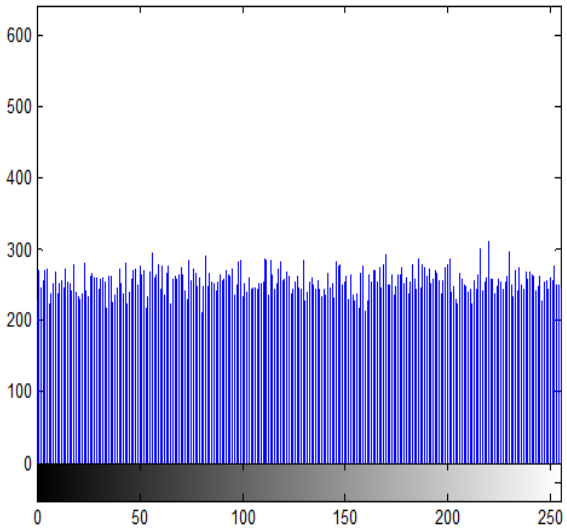
(a)




(b)



(c)

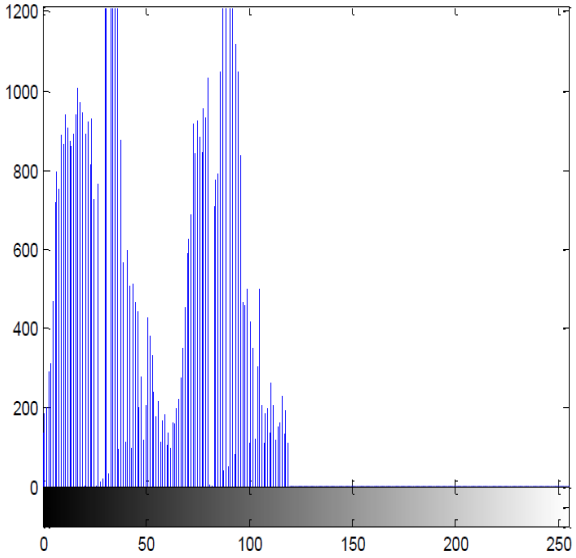



(d)

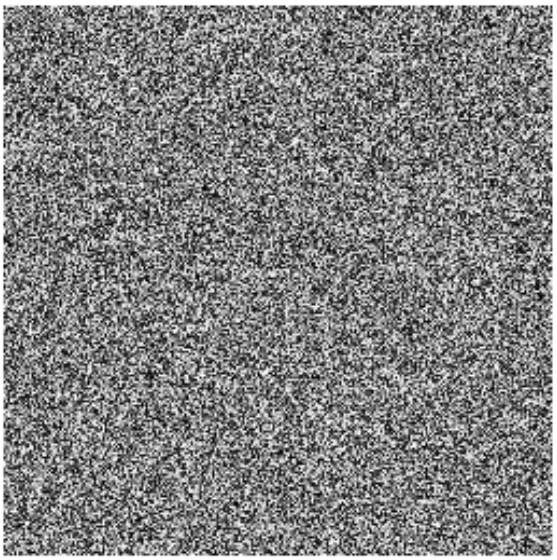
*Figure 4: (a) MRI Image. (b) Histogram of MRI image. (c) Encrypted Image. (d) Histogram of Encrypted Image.*

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

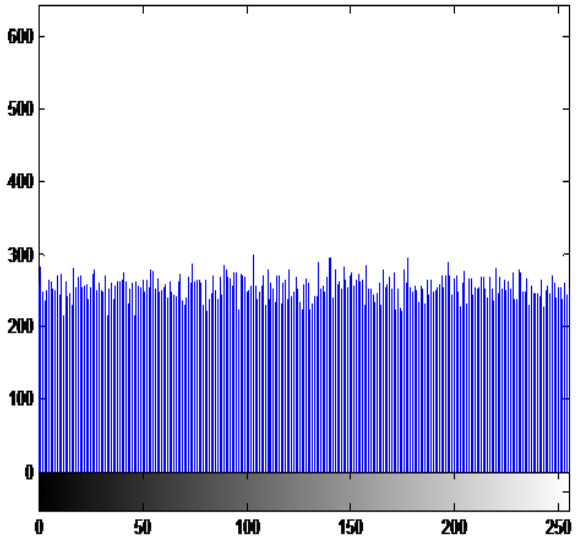
(a)




(b)



(c)




(d)

*Figure 5: (a) WOMAN Image. (b) Histogram of WOMAN image. (c) Encrypted Image. (d) Histogram of Encrypted Image*