International Journal of Advanced Science and Technology
Vol.121 (2018), pp.43-54
http://dx.doi.org/10.14257/ijast.2018.121.04

Review of Different Image Data Hiding Techniques

Sonali Mishra[1], Ananya Dastidar[2*], Umesh Chandra Samal[3] and Sushanta Kumar Mohapatra[4]

[1,2]*Department of Instrumentation and Electronics, College of Engineering and Technology, Bhubaneswar, Odisha, India*
[3,4]*School of Electronics Engineering, Kalinga Institute of Technology, Bhubaneswar, Odisha, India*
[1]*sonalimishra135@gmail.com* [2]*adastidar@cet.edu.in*
[3]*umesh.samalfetr@kiit.ac.in* [4]*skmctc74@gmail.com*

Abstract

With the rapid progress of diverse communication technologies and the prevalence of computer and network technology, it is a big challenge to ensure secure transmission of information from source to destination. The World Wide Web is used as a medium to circulate a huge amount of digital information throughout the world every day. Most of these data contains valuable information that face the threat of being exposed and being corrupted. Encryption methods are evolving which is moving towards a future of limitless possibilities. Cryptography denotes the storing and transmission of information in a specific way so that the owner of the key only can access and process it further. This paper presents the study of different encryption and decryption techniques used for storing and transmitting of data and also implements the watermarking techniques and cryptography for study of encryption. We also propose a hybrid encryption technique based on watermarking and cryptography-the Secure Force Algorithm. The proposed hybrid technique gives us a promising result in terms of its mean square error and peak signal to noise ratio.

Keywords*: Cryptograph; Decryption techniques; Encryption techniques; Steganography; Watermarking*

1. Introduction

Today Security of Data has gained a lot of importance for all types of communication system. Extensive use of images, the text had made it more significant to focus on the area of data security. While the relentless use of Internet and Communication Technology is unavoidable, in the use of data sharing, many ways to provide security to data, are also being developed to look into the issues related to hacking, unethical sharing, etc. This paper reviews different literature based on various techniques used for data security in the field of communication. Image encryption is a method that sends out the image securely over various data communication networks to prevent the access of the secret information from illegal users. Some of the features of the image are its size, redundant nature and pixel correlation, which make it distinct from other data. Encryption techniques are well considered and very beneficial tool to protect the secret and valuable information from unauthorized and illegal users. Encryption converts the plain message to ciphertext which cannot be accessed by any unauthorized users. Decryption converts encrypted data to its original data form to make it accessible to the users. These techniques include encryption

Received (September 2, 2018), Review Result (November 3, 2018), Accepted (November 9, 2018)
*Corresponding Author

ISSN: 2005-4238 IJAST

and decryption of the data- image, video, audio, and text. The internet communication, medical imaging, transmission are the fields where image encryption, video encryption, chaos-based encryption have their purposes. Examples are; Tele-medicine, military Communication, etc. Digital watermarking along with cryptography are also another method that has been proposed and studied over the years as one of the possible ways to deal with this problem. Watermarking protects its ownership of the data to be transmitted. On the other hand, the cryptography provides the security for the reliable communication of the transmitted message over the communication channel, which also protects the useful information content of the data thereby making it possible for only the authorized person to access the information.

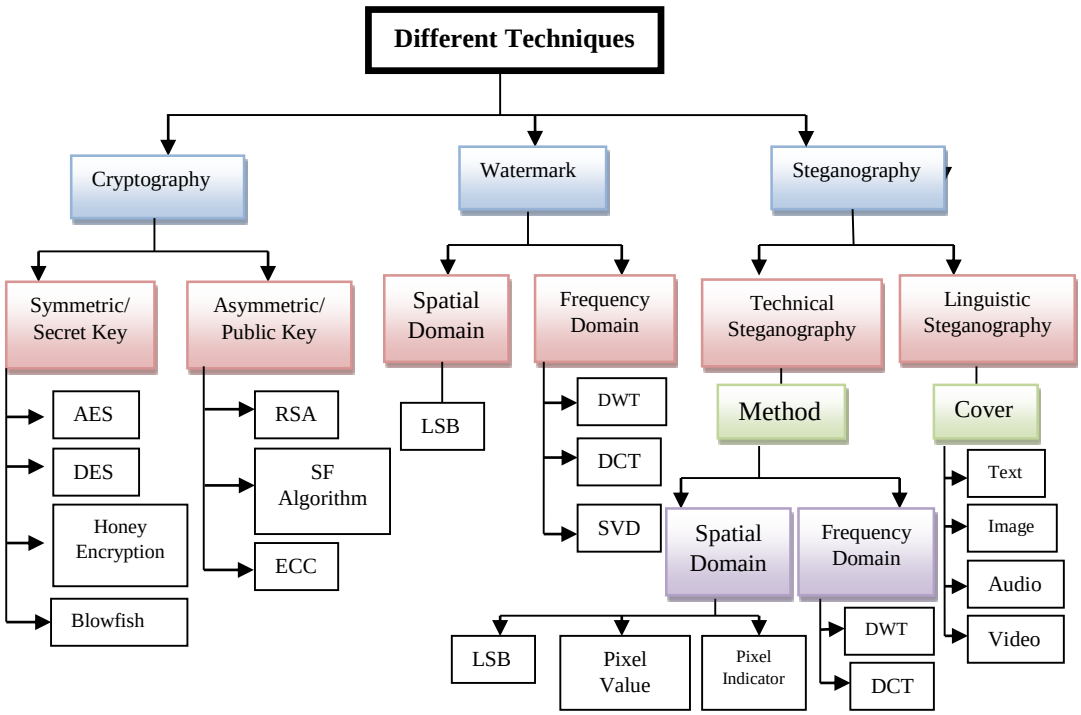

Figure 1. Classification of Different Techniques used for Security Purpose

Digital multimedia content must be protected, secured and authenticated during transmission to make the Quality-of-Service (QoS) better for any communication systems. The various researcher has been contributed remarkably in the field for secure the data during transmission from unauthorized users. Still, it is one of the recent and open challenges for researchers and industries as the field of communication and networking developing tremendously in a faster way in recent years and continue to be in the future years.

In this paper, we have focused on various types of data encryption, and description techniques, their advantages, limitations and its specific applications in different field like message, text and image and video data transmission are discussed in detail. Some of the recent or existing techniques such as digital watermarking and SF algorithm are implemented and compared with the proposed hybrid one.

The various methods used for security purpose can be seen in Figure 1. The classification includes Watermark Technique, Cryptography Technique and Steganography Technique. These techniques can be used for increasing the information safe and can prevent data theft and/ or corruption. The paper starts with a section containing the literature on different encryption and decryption algorithms for different types of data such as text message, video, and image. This is followed by a brief idea on the various techniques for encryption. Some simulation result for encryption has also been

presented herein.

2. Encryption and Decryption Algorithms

In this section, various types of encryption and decryption algorithm developed by various authors are discussed, with its specific application in the field of communication and networking.

2.1 Cryptography

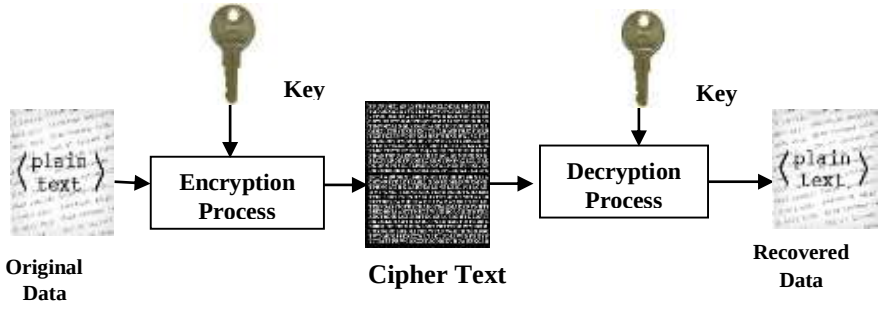

Figure 2. Basic Model of Cryptography

Reliability and security in data communication is gaining importance in an increasingly multimedia defined world nowadays. Cryptography makes a cryptosystem which provides security to the information for the secure and reliable data transmission.

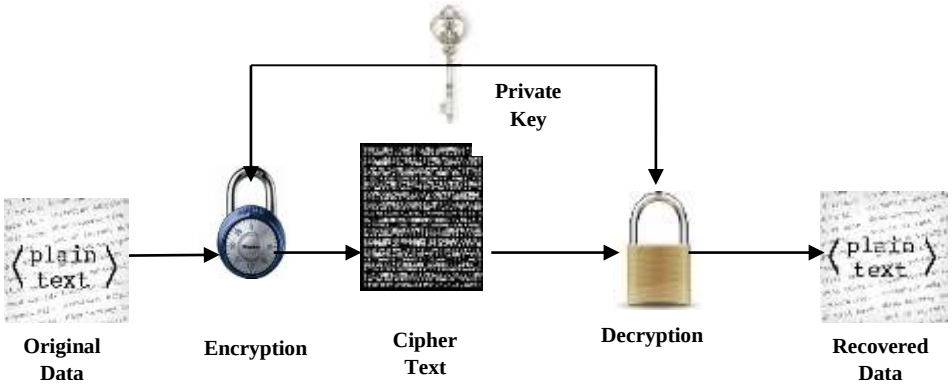

Figure 3. Private/ Symmetric Key

The different constituents of basic cryptosystem are; text or the message signal which is to be protected before transmission over the communication channel, data encryption algorithm, ciphertext, data decryption, the encryption and decryption keys. Encryption is a process which encodes the data in a method such that it becomes accessible only by an authorized person.

The ciphertext is the jumbled version of the plain text (data) which is created by using a specific encryption key which is again generated by the encryption algorithm. It flows on the public channel. Decryption algorithm produces a unique plain text for any given ciphertext and decryption key. The encryption key or sender and the decryption key or receiver is the source and destination of the system respectively [1].

There are two types of key used which are carried out by encryption-decryption. First is the Symmetric Key wherein both encryption and decryption keys are equal while the other is the Asymmetric Key wherein only the encryption key is published for everyone to use but the decryption key is not published to everyone [2].

While the symmetric key is also called the public key while the asymmetric key is also known as private key. Figure 3 and 4 show how a Private and a Public key based encryption models look like. We now will look into different encryption algorithms.

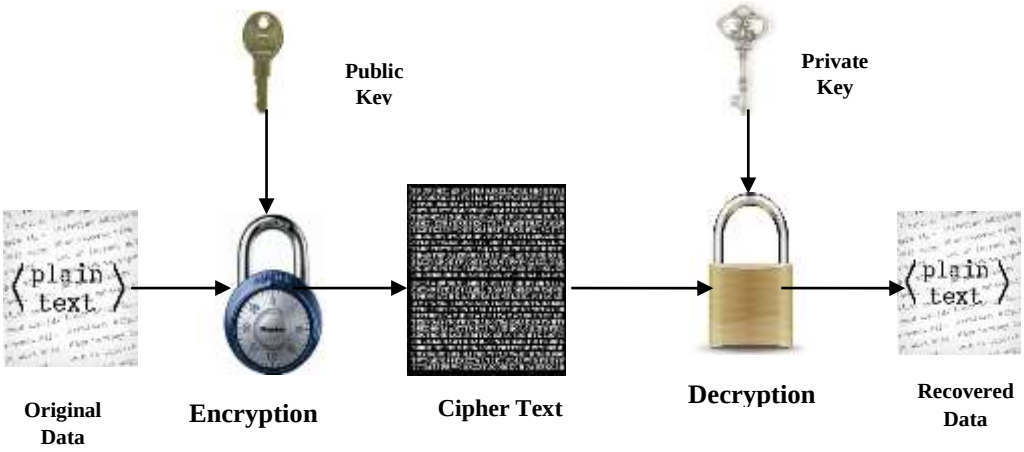

Figure 4. Public/ Asymmetric Key

2.2 Encryption using Advanced Encryption Standard (AES) Algorithm

Rijndael is an arrangement for the encryption information [3]. The National Institute of Standards and Technology (NIST) started progress of AES in 1997 when it declared require for a successor algorithm for the DES, which was started to be converted into vulnerable to brute-force attacks. So, DES is substituted by AES. The AES algorithm describes some changes that are to be performed on information which is accumulated in an array. The 1st stage of the cipher is to place the information into an array, and then the cipher changes recur over some encryption rounds. By the key length the number of rounds is determined; get 128-bit keys from ten rounds, 192-bit keys from twelve rounds and 256-bit keys from fourteen rounds.

AES algorithm has found wide use in encryption for transmission of digital data. Many literatures have proposed an improvement in the AES algorithm to reduce the effects of Brute-Force attacks, unwanted channel snooping and illegal data access. In [4] Fathy a *et.al*. have discussed the issues and implementations of the AES algorithms are faced as data to be transferred is diverse, vast and may require remote exchange. Sensitive data transmission takes place every day on different channels which can be well comprehended from the amount of traffic on e-commerce and banking channels. AES remains the main focus of research for implementations in different domains. AES finds its use in Machine Learning, IoT applications [5], Satellite Imaging [6], SMS encryption [7] *etc*.

A video encryption based on AES algorithm to protect unnecessary interception and analysis of any video at the same time as in to communicate over the networks have been implemented that allowed protected end-end (point to point or point to multi-point) data communication over the network [8]. Digital watermarking faces some tough difficulties for practical uses. However, there were no other techniques available which will substitute it. FPGA implementation of AES by for numerous trade-off between area and speed to suit a range of application was seen [9]. Efficient, secure communication with network cryptographic methods compared to other techniques was also debated.

2.3 Encryption using Data Encryption Standard (DES) Algorithm

It is a symmetric-key algorithm as it uses a unique key for both the encryption and decryption. DES is now regarded to be insecure because the possible of brute force attack. The DES is a block cipher that encrypts an n-bit block of plaintext using a key to produce

an n-bit block cipher text. The key is represented as an n-bit block from which an effective key is generated for encryption and decryption. In 64-bit key value, every bit is parity bits used for parity checking which are discarded and contain no effect on DES's security [10]. The main difference between the DES encryption and DES decryption is that the sub-keys are supplied in reverse order. The security strength of the DES algorithm considers the various attacks such as Brute-force, differential and linear cryptanalysis [11]. In DES algorithm, the size of the key is 64 bits and so that it can encrypt only 64-bit plaintext at a time. It is necessary to divide the message into 64-bit block of data so that it can be encrypted a plaintext message which is larger than 64 bits. Each 64-bit message can be encrypted using the same 64-bit key value using DES encryption operation.

Secure Cryptosystem is the fundamental to high speed computing. The length of the key length and the network (feistel) are worked upon for modification of the DES algorithm for making it more resistant to crypto-attack. In [12] Verma et.al., have proposed a similar modification that divides the n bits of right block into two equal blocks of n/2 bits on which two varied functions are applied and the effective key length is also increased. The performance was then compared to standard DES. Image steganography based on DES was reported in [13]. Use of DES in increasing the security of Smart Cards has also being reported [14].

2.4 Data Encryption and Decryption Using Rivest, Shamir and Adleman (RSA) Algorithm

The encryption public key in RSA is distinct from the decryption private key [15]. In [16] Nentawe Y. Goshwe reported a data encryption/ decryption technique using RSA in a network environment, which has a precise size (block) of the message. The message sender is permitted to produce public keys for the encryption while the private key is sent to the receiver using secured database. A private key which could be erroneous would still able to decrypt the encrypted message. However, it is different from the original message. In [17] Md. Ashraful Islam et.al., implemented a secure asymmetric RSA encryption and description for the transmission of a text message in wireless communication systems. The RSA algorithm was implemented and well accepted for public-key encryption. Mohammed A. Saleh *et al* have presented a comparative analysis between DES, RSA and AES encryption algorithm [18]. They decided that which algorithm may be suitable to transfer the video data safely with keeping the balance between the computational complexity and security of the data. To convert the original data to encrypted data, they used encryption process so that the original data can be recovered from the encrypted data by using proper decryption process.

2.5 Data Encryption and Decryption using Honey Encryption (HE) Algorithm

A novel encryption technique generates a cipher text that gives an erroneous plaintext password when the attacker tries to decrypt the data by guessing a wrong key. The HE security depends on the fact that the possibility of an attacker thinking a plaintext to be legitimate can be calculated during encryption by the encrypting party. This makes HE difficult to be used in certain applications, *e.g.*, where the space of plaintext is very huge or the allotment of plaintext is not known. It also means that HE can be in danger due to brute-force assaults if this probability is calculate wrongly. For example, it is susceptible to known-plaintext attacks *i.e.*, if the attacker has a copy that must be equivalent to a plaintext to be legitimate, they will be able to brute-force even HE data if the encryption did not take the copy into account [19].

2.6 Data Encryption and Decryption using Secure Force (SF) Algorithm

Wireless sensors used in WSN are small in size. Some of the resources required for the WSN such as power available to the sensors and limited computational facilities are some of the constraints need to be taken into consideration. Due to the limited computational facilities available to the sensor nodes, some of the power efficient methods are developed for mathematical operations. This method can help to bring down the toll on the encoder and make it power efficient due to low computational complexity. The complex key expansion at the decoder is also seen [20]. The SF algorithm can be designed in such a manner that the complexity can be reduced and more power efficient which can be implemented suitably for the encryption of WSN data. Data confusion and diffusion process provide different resistance types of attacks. Translation, scaling, rotation and shearing are some affine transformations. SF algorithm with Affine Transform for image encryption was seen in [21], [22]. It is an asymmetric algorithm, and its computational complexity is also low which may be beneficial for real-time encryption of the image for secure transmission. Here the correlation among image pixels are removed with the help of random chaos sequences using ADD and XOR functions.

2.7 Digital Image Watermarking

Digital watermarking has been put forward to deal with this problem, to keep information safely. For intellectual property rights protection the digital watermarking has become very popular approach.

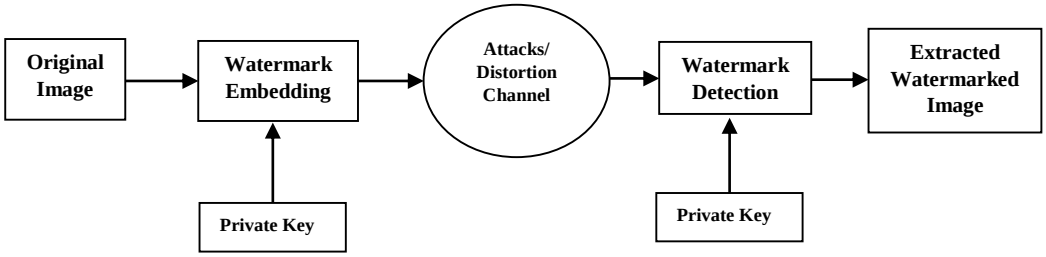

Figure 5. Basic Procedure of Digital Image Watermarking

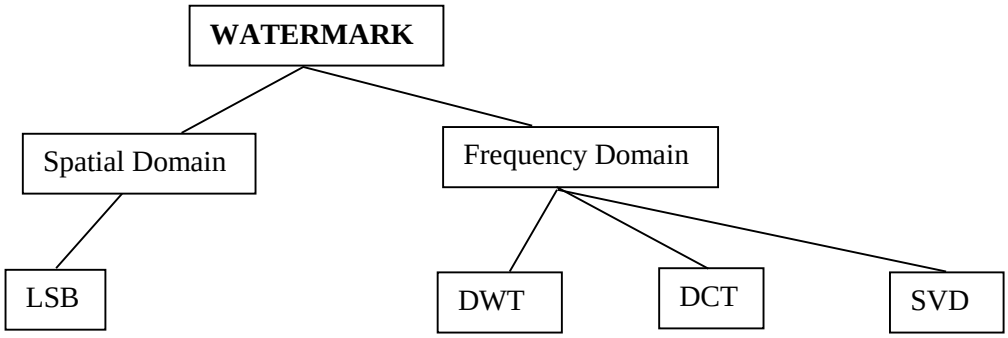

Figure 6. Types of Watermark

Different types of watermarking techniques and a large number of processes were proposed, but still most of the known ways which are protected the data. By the watermarking procedure these text, images, audio, and video can be processed. To be able to prove the ownership, the owner must hide the data within the material which should be published. The watermark should be unnoticeable for unauthorized user. It should not affect to an original data quality and should be tough against different types of attacks [23]. It is widely spread in the several kinds of applications which have a lot of informative data. Classification of Watermarking can be seen in Figure 6 below.

H. Liu *et. al* have reported a method for image encryption and watermark detection in the encrypted/ decrypted domain. They have used encryption based on Compressive Sensing, watermarking based on the Scalar Costa Scheme [24].

VLSI implementation of digital image watermarking has also being reported in various literatures. In order to understand the power capability, performance characteristics and reliability of the digital watermarking algorithm, a hardware implementation of the same was proposed [25]. Implementation of both fragile and robust watermarks in the image was reported.

2.8 Steganography

Steganography is closely related to cryptography. In cryptography, messages are scrambled so that nobody can understand the message. On the other hand in steganography messages are hidden so that the existence of the message can not be determined [27]. Use of a type of steganography for covert channel communication to achieve data hiding without compromising on quality has also been studied [28]. Masoud Nosrati *et.al.*, introduced the different methods such as audio, text and image steganography used for encryption considering the cover data [29]. Figure 7 above shows different steganography methods that have been studied and/ or implemented in various literatures.

2.9 Hybrid techniques for Encryption

A Kaur *et al*, have presented a novel hybrid algorithm for the transmission of text message securely over the communication channel [30]. The hybrid scheme was based on XOR cipher, PN sequence, Hill cipher, Fibonacci series, RSA, one bit, two bit and three bit least Significant Bit (LSB). They evaluated the quality of watermarked images concerning MSE, RMSE, and PSNR. Hybrid cryptographic methods for encryption of image can be used to improve the level of security and also to study their amalgamation hybrid cryptographic techniques which combine the digital watermarking and cryptography [30]. A hybrid implementation using Blowfish and RSA algorithm was proposed in [31] for cloud applications where authentication was primarily carried out using digital signatures. The technique presented in this paper contains the features of both asymmetric and symmetric cryptography. The FPGA implementation of this system was also reported. Regarding security, a hybrid approach has been found to provide more secure encryption and pose a deterrent to hackers.

Use of Wavelet Function for encryption of grayscale images was proposed in [32] where the Discrete Meyer wavelet function has been shown to give high compression ratio and the improved PSNR (peak signal to noise ratio) value for an encrypted grayscale image. Another hybrid technique for Secure Data Communication using data hiding and Image Encryption is based on two technologies- Reversible Data Hiding and the Hyper (Hash) Image Cryptography was proposed in [33].

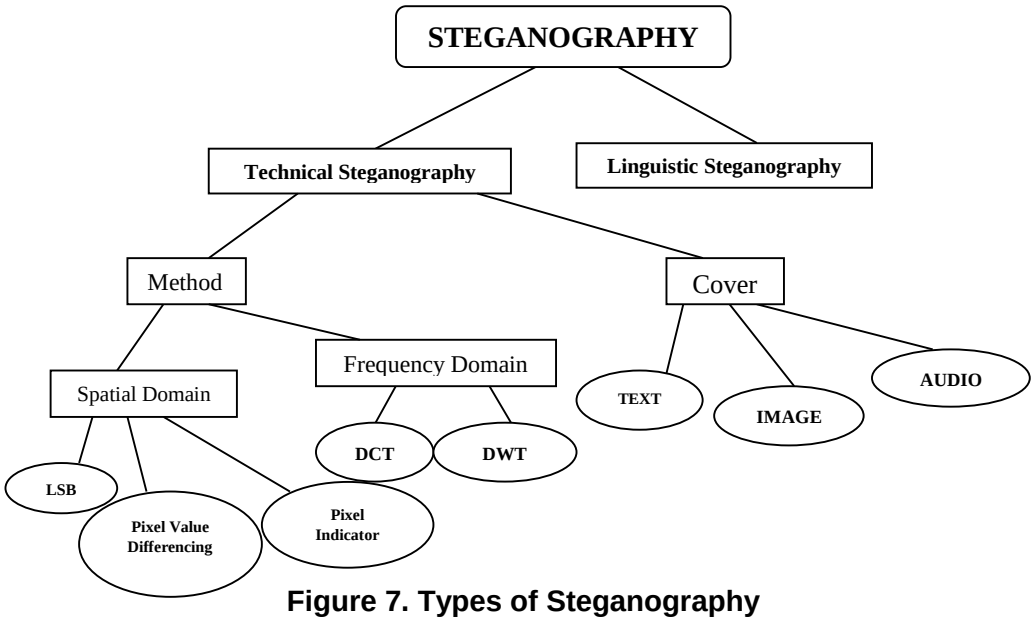

Figure 7. Types of Steganography

3. Result and Discussions

Here we have used an image as data and for this we have taken the MATLAB standard Lena image. Firstly, we apply encryption to the image by using watermark technique which is followed by encryption of the same image by using cryptography technique.

Figure 8. Original, Attacked, the Recovered Image of Lena Using Blurred Watermarking

Further we encrypt that data image by hybrid technique which is implemented by using both watermarking and cryptography technique. Finally we make a comparative study between them. Figure 8 shows the original, attacked and recovered image by using the only watermarking technique. Here the blurred image is watermarked image where some attacks present which is a blur.

Figure 9. Original, Encrypted, Decrypted Image of Lena Using SF Algorithm

Figure 9 shows original, encrypted and decrypted image by using SF algorithm. Here the encrypted image can not show any image of Lena which is hidden in the encrypted image. The different parameters calculated for the above two techniques can be seen Table 1 later.

Many hybrid techniques are being implemented using different techniques. In this paper we develop a hybrid technique by using both Watermarking and Cryptography (Secure Force algorithms) for encryption.

Figure 10. Implementation of the Hybrid Technique

Figure 10 and 11 shows the original, embedded, encrypted and decrypted image of Lena by using hybrid process. The original image and decrypted image is almost same which means the image is not corrupted. In the hybrid algorithm, we used both watermark technique and SF algorithm to get a better result.

Table 1. Calculation of MSE, PSNR, and SNR of Different Algorithms

Algorithms	MSE	PSNR (dB)	SNR (dB)
Only Watermarking	0.22	54.70	13.97
Watermarking [25]	-	-	20-25
Only SF Algorithm	35.56	39.38	13.77
SF Algorithm [21]	541.48	-	10.79
Hybrid Technique (Watermarking and SF Algorithm)	50.92	31.10	13.68
Hybrid Technique [34]	57.56	56.93	-

Table 1 shows the calculation of Mean Square Error (MSE), Peak signal-to-noise ratio (PSNR) and Signal to Noise Ratio (SNR) values of different algorithms.

Mean Square Error (MSE) is defined as the average of the squared error values between the actual and decrypted image values. MSE between the original and decrypted images is computed as,

$$\mathrm{MSE} = \frac{1}{\mathrm{M}*\mathrm{N}} \sum_{\mathrm{i}=0}^{\mathrm{M}-1} \sum_{\mathrm{j}=0}^{\mathrm{N}-1} \left| \mathrm{f}(\mathrm{i},\mathrm{j}) - \hat{\mathrm{f}}(\mathrm{i},\mathrm{j}) \right|^2 \quad (1)$$

Where M and N represent the dimension of the image data while $\mathrm{f}(\mathrm{i},\mathrm{j})$ and $\hat{\mathrm{f}}(\mathrm{i},\mathrm{j})$refers the original and decrypted images respectively. It is a useful measure for the average energy lost in the lossy compression of the original image data. A very small MSE value may be interpreted as the decrypted image to be very close to original image data.

The ratio of the signal power to noise power is given by the signal-to-noise ratio (SNR).

$$\mathit{S}\mathrm{NR} = 10 \log_{10} \left[\frac{\sum_{\mathrm{i}=0}^{\mathrm{M}-1} \sum_{\mathrm{j}=0}^{\mathrm{N}-1} \hat{\mathrm{f}}(\mathrm{i},\mathrm{j})^2}{\mathrm{MSE}} \right] \quad (2)$$

The ratio of the peak signal power to noise power is given by the peak signal-to-noise ratio (PSNR). It is a measure the quality of reconstructed images that has undergone

compression. The colour value of each pixel in an image undergoes changes due to compression and decompression. PSNR is expressed in in decibels, given as,

$$\text{PSNR} = 10 \log_{10} \frac{(255)^2}{\text{MSE}} \quad (3)$$

Here we take watermarking technique, SF algorithm, and hybrid technique and get different values of MSE, PSNR, and SNR. When different techniques was applied to the data image the MSE was found to be SNR was found to be 13.97 for watermarking, 13.77 for SF algorithm, and 13.68 for hybrid technique as seen in the table above. Although Watermarking produces a lower MSE but it lacks the security provided by cryptography. So by using a hybrid technique we can include the advantages of both the watermarking and cryptography. The proposed hybrid technique gives a better result with reference to other hybrid technique in terms of both MSE and PSNR.

4. Conclusion

Security is a major concern in various domains like forensics, trade market, medicine, banking, militia, census to name a few. In order to conceal the information in the data contains, data hiding techniques are employed to maintain the confidentiality of the same. In this paper, different techniques for image, text, video encryption and decryption have been studied. Many literature are available that has implemented different encryption, decryption and hybrid techniques. Most of these techniques are useful for real-time encryption. These techniques allow us to keep our image, audio, text, and video safe. In this paper we proposed the use of two different algorithms- watermarking and Cryptography (Secure Force (SF) algorithm) and made a comparative study between them. We also proposed a hybrid technique by using these two algorithms to get better results. The Mean Square Error of the Hybrid techniques gave the best result among the three techniques. So we can claim that hybrid encryption schemes will deliver better performance than simple implementations. On a daily basis, new encryption methods are established hence quick and more protected encryption methods will constantly give out a high rate of safety. Depending on the application domain the algorithms maybe further studied for implementation. From the different implementation and after comparison with previous literature we conclude that experiments we can conclude that, the hybrid technique gives a better result regarding the closeness of the decrypted image to the original image data when compared to other techniques. Use of hybrid techniques includes the advantages of both the algorithms thereby making the approach more secure.

References

[1] J. A. Buchmann, “Introduction to Cryptography”, Springer **(2008)**.
[2] M. Bellare, A. Boldyreva, S. Micali, “Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements”, Advances in Cryptology- EUROCRYPT 2000, Lecture Notes in Computer Science, vol 1807, Springer, Berlin, Heidelberg; **(2000)**.
[3] Daemen, Joan, Rijmen, Vincent, “AES Proposal: Rijndael”, **(1999)**.
[4] A. Fathy, I.F. Tarrad, H.F.A. Hamed, A.I. Awad, “Advanced Encryption Standard Algorithm: Issues and Implementation Aspects”, Advanced Machine Learning Technologies and Applications. AMLTA 2012, Communications in Computer and Information Science, vol 322. Springer, Berlin, Heidelberg; **(2012)**.
[5] M. E. Hameed, M. M. Ibrahim, N. A. Manap, “Review on Improvement of Advanced Encryption Standard (AES) Algorithm based on Time Execution, Differential Cryptanalysis and Level of Security”, Journal of Telecommunication, Electronic and Computer Engineering (JTEC), vol. 10, no. 1, **(2018)**, pp. 139-145.
[6] F.T.B. Muhaya, “Chaotic and AES cryptosystem for satellite imagery”, Telecommunication Systems, February 2013, vol. 52, no. 2, **(2013)**, pp. 573–581.
[7] S. Ariffi, R. Mahmod, R. Rahmat, N. A. Idris, “ SMS Encryption Using 3D-AES Block Cipher on Android Message Application”, International Conference on Advanced Computer Science Applications and Technologies, 2013, Kuching, Malaysia, IEEE, **(2014)**.

[8] D. M. Dumbere and N. J. Janwe, "Video encryption using AES algorithm", Second International Conference on Current Trends in Engineering and Technology - ICCTET 2014, Coimbatore, **(2014**), pp. 332-337.
[9] M.D. Rahane and S.M. Turkane, "FPGA Secured wireless communication using AES", International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622, vol. 3, no. 4, **(2013)**, pp. 2404-2407.
[10] W. E. Burr, "Data Encryption Standard, in NIST's anthology A Century of Excellence in Measurements, Standards and Technology", A Chronicle of Selected NBS/NIST Publications, 1901-2000.
[11] D.Coppersmith, "The data encryption standard (DES) and its strength against attacks at the Wayback Machine", IBM Journal of Research and Development, vol. 38, no. 3, **(2007)**, pp. 243-250.
[12] J. Verma and S. Prasad, "Security Enhancement in Data Encryption Standard", Information Systems, Technology and Management, ICISTM 2009, Communications in Computer and Information Science, vol 31. Springer, Berlin, Heidelberg, **(2009)**.
[13] M. K. Ramaiya, N. Hemrajani and A. K. Saxena, "Improvisation of security aspect in steganography applying DES", IEEE, **(2013)**.
[14] A.M. Sison, B.T. Tanguilig, B.D. Gerardo and YC. Byun, "Implementation of Improved DES Algorithm in Securing Smart Card Data", Computer Applications for Software Engineering, Disaster Recovery, and Business Continuity, Communications in Computer and Information Science, vol. 340. Springer, Berlin, Heidelberg, **(2013)**.
[15] G. Prashanti, S. Deepti and K Sandhya Rani, "A Novel Approach for Data Encryption Standard Algorithm", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958, vol. 2, no. 5, **(2013)**, pp. 264.
[16] N.Y. Goshwe, "Data encryption and decryption using RSA algorithm in a network environment", IJCNCS, vol.13, **(2013)**.
[17] A. Islam and A. Z. M. Touhidul Islam, "Secure wireless text message transmission with the implementation of RSA cryptographic algorithm", IJCNCS, vol.2, **(2014)**.
[18] M. A. Saleh, N. Md. Tahir, E. Hisham and H. Hashim, "An analysis and comparison for popular video encryption algorithms", IEEE, Selangor, Malaysia, **(2015)**.
[19] A. Juels, T. Ristenpart, "Honey Encryption: Security Beyond the Brute-Force Bound", Advances in Cryptology – EUROCRYPT 2014, Lecture Notes in Computer Science, vol. 8441. Springer, Berlin, Heidelberg, **(2014)**.
[20] W.K. Koo, H. Lee, Y.H. Kim, and D. H. Lee, "Implementation and analysis of new lightweight cryptographic algorithm suitable for WSN", International Conference on Information Security and Assurance, IEEE, **(2008)**.
[21] P. Lakshmi Sowjanya, K.J. Silva Lorraine, "Image Encryption Using Secure Force Algorithm with Affine Transform for WSN", International Journal Of Engineering Sciences & Research Technology, August, vol. 5, no. 8, **(2016)**, pp. 379-387.
[22] J. Ahmad and S.O. Hwang, Multimed Tools Appl , "A secure image encryption scheme based on chaotic maps and affine transformation", Multimedia Tools and Applications, vol. 75, no. 21, **(2016)**, pp. 13951-13976.
[23] C.I. Podilchuk, E.J. Delp, "Digital watermarking: Algorithms and Applications", IEEE Signal Processing Magazine, **(2001)**, pp.33-46.
[24] H. Liu, D. Xiao, R. Zhang, Y. Zhang, S. Bai, "Robust and hierarchical watermarking of encrypted images based on compressive sensing", Signal Processing: Image Communication, Elsevier, vol. 45, **(2016)**, pp 41-51,.
[25] S. P. Mohanty, N. Ranganathan and R. K. Namballa, "VLSI implementation of invisible digital watermarking algorithms towards the development of a secure JPEG encoder", IEEE Workshop on Signal Processing Systems (IEEE Cat. No.03TH8682), **(2003)**, pp. 183-188.
[26] R. Krenn, "Steganography and steganalysis", Internet Publication, **(2004)**, Available at:http://www.krenn.nl/univ/cry/steg/article.pdf.
[27] D. Artz, "Digital steganography: hiding data within data", IEEE Internet Computing, vol. 5, no. 3, **(2001)**.
[28] M. Amiruzzaman, H. Peyravi, M. Abdullah-Al-Wadud, Y. Chung, "Covert Channel Communication by Betterment Steganography", International Journal of Multimedia and Ubiquitous Engineering, vol. 5, no. 3, (**2010**), p. 1.
[29] M. Nosrati, R. Karimi and M. Hariri, "An introduction to steganography methods", World Applied Programming, vol.1, **(2011**).
[30] A. Kaur and S. Singh, "A hybrid technique of cryptography and watermarking for data encryption and decryption", 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), Waknaghat, (**2016)**, pp. 351-356.
[31] V. P. Bansal and S. Singh, "A hybrid data encryption technique using RSA and Blowfish for cloud computing on FPGAs", 2015 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS), Chandigarh, **(2015)**, pp. 1-5.

[32] S. Suresh Kumar, H. Mangalam, "Wavelet-based Image Compression of Quasi Encrypted Grayscale Images", International Journal of Computer Applications (0975- 8887), vol. 45, no.12, **(2012)**, pp. 35-39.
[33] Ȧ. Sowmyashree and R.R. SedamkarȦ , "A Hybrid Approach for Secure Data Communication using Reversible Data Hiding and Image Encryption", International Journal of Current Engineering and Technology, **(2014)**, pp. 4226-4233
[34] C. Yoga Anitha, P. Prabhu, "Complexity Analysis of Hybrid Method for Securing and Compressing Images", International Journal of Pure and Applied Mathematics, ISSN: 1314-3395, vol. 119, no. 15, **(2018)**, pp 2221-2230.

