DOI: http://dx.doi.org/10.26483/ijarcs.v8i8.4848

ISSN No. 0976-5697

Volume 8, No. 8, September-October 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A REVIEW ON COMBINED SCHEMES TO ENCRYPT AND COMPRESS DIGITAL IMAGES

Priya Yadav
Department of Computer Engineering and Application
National Institute of Technical Teachers' Training and ResearchBhopal, M.P, India

R.K Kapoor
Department of Computer Engineering and Application
National Institute of Technical Teachers' Training and ResearchBhopal, M.P, India

Abhinn Pandey
Department of Computer Engineering and Application
Institute of Technical Teachers' Training and Research
Bhopal,M.P, India

***Abstract*:** Encryption plays an important role to guarantee classified transmission of information over web. Over the years images have emerged as one of the most widely used forms of communication. Various methods have been developed at spatial, frequency and hybrid domains for image encryption. Commonly to transmit information faster over network compression is used. Recently there have been advancements in combining encryption and compression together. In these paper techniques for application of combined encryption and compression over digital images proposed over recent years have been surveyed. This paper also points out some of the future directions which may lead to new path to improve current models.

Keywords: Image encryption, Image compression, Data Hiding, DCT, JDHC, PSNR, CRT.

I. INTRODUCTION

Over recent years, rapid growth in transmission of information over public network has raised lot of interest over data security. Image being one of the common and most widely used forms to transmit information have attracted massive interest in communication security.

Image compression is the process of encoding or converting an image file in such a way that it consumes lesser space than original file. Compression is used to reduce the redundancy of data without affecting its quality. Compression also reduces the time required for images to be sent over the internet or downloaded from web pages. There have been various enhancements in compression techniques.

Classification of compression:

1-Loseless Compression

2-Lossy Compression

Lossless Compression: In lossless compression there is no loss of information. If data has been losslessly compressed then original data can be recovered without any loss of information.

Lossy Compression: In lossy compression some information may get lost while compressing the data. Lossy compression focuses on saving space over preserving the accuracy of data.

Encryption [1] can be defined as converting plain data which can be read easily to cipher data which cannot be read by any user without decrypting it. Decryption [1] can be defined as reverse process of encryption that is converting cipher data to plain data.

Image encryption has serious intimidation for transmission as many domains like medical data, military data, celestial information etc. have much information in the form of images and mainly these domains require high confidentiality while transmitting or storing information. Over recent years many new studies as well as advancements in pre-existing methods have been performed to make image transmission more secure and faster. This paper lists some of the recent works as well as advancements in this field.

This paper has been organized in following sections. First section, gives general overview of compression, encryption, cryptography and terms generally used in them. Second section, discusses contemporary advancements in cryptographic methodologies. Last section summarizes the study and discusses future directions to improve upon current models.

II. OVERVIEW OF CRYPTOGRAPHY

A. Preliminaries

1. Plain Text

The original message that the person wishes to communicate with the other is defined as Plain Text. For example: if a person has "hello, how are you?" as message to be sent then this message is categorized as pain text.

2. Cipher Text

The message that cannot be understood by anyone or has been deliberately made meaningless to hide original message is what we call as Cipher Text. For example, "Ajd672#@91ukl8*^5%" is a Cipher Text that might be produced for "Hello Friend how are you".

3. Encryption

A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. The process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.

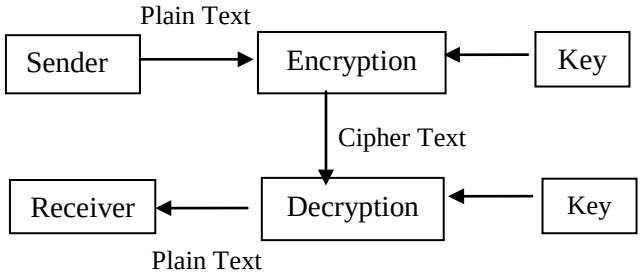

Figure 1:. Process of cryptography.

4. Decryption

A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from Cipher Text. The process of decryption requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption.

5. Key

A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it.

The process of encryption can be represented as shown in Figure 1, the original message or plain text at senders' side is first encrypted using key. Then the cipher text hence generated, is transmitted over network to receiver there cipher text is first decrypted using key then the message is read by receiver as plain text.

B. Goals of Cryptography

Following are the goals of cryptography.

- Confidentiality: Information must be accessed by authorized user only.
- Authentication: The information received by any system must check the identity of sender to access whether the information is arriving from an authorized perrson or not.
- Integrity: Only authorized user is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.
- Non-Repudiation: Ensures that neither the sender, nor the receiver of message should deny the transmission.
- Access Control: Only the authorized parties are able to access the given information.

C. Classification of Cryptography

Encryption algorithms can be classified into two broad categories - Symmetric and Asymmetric key encryption.

• Symmetric Key Cryptography

In symmetric key cryptography, the key used for encryption is similar to the key used for decryption. Thus, the key distribution is made prior to transmission of information. There are various symmetric key algorithms such as DES, 3DES, BLOWFISH, Twofish, AES, RC4 etc.

• Asymmetric Key Cryptography

In asymmetric key cryptography or public-key cryptography a pair of keys namely public key and a private key are used. Any user who wants to send an encrypted message can get the intended recipient's public key from public directory and use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key. That is using public key any one can encrypt but decryption is possible only by using private key.

The image encryption algorithms can be classified into three major groups:

1. Position permutation based algorithm [2]
2. Value transformation based algorithm [3, 4]
3. Visual transformation based algorithm [2].

III. LITERATURE REVIEW OF IMAGE ENCRYPTION TECHNIQUES

To make transmission faster and secure, recently use of compression and encryption has attracted vast attention. Encrypting multimedia using conventional cryptographic techniques is termed as naive approach. Currently researches focus upon joint encryption and compression scheme this refers to as selective encryption [5].

A. Chaos based joint image compression and encryption using DCT and SHA-1.

As authors in [6] have mentioned, the DCT [7] (Discrete cosine transformation) has presented a commonly used popular way to compress an image due to its strong energy compaction property. But it doesn't guarantee confidentiality while transmitting. Recently many authors [8], [9] have worked with joint compression and encryption techniques to incorporate confidentiality with fast transmission of information. Further extending those works author [6] has modeled an approach using chaos based approach with SHA-1 for encryption and DCT for compression. The results hence obtained are compared with another model created using DCT, Huffman coding and AES on Aerial, Baboon, Barb, Frog, Gold hill, Sailboat. It was observed that proposed approach suffered degraded compression performance. Proposed approach performed faster as compared to compression followed by AES. Though key space was found to be same, but due to randomness in proposed model due to chaos based model incorporation, key is found secure as it can be cracked using brute-force search only. It has also been affirmed that proposed model has high key sensitivity and pain-image sensitivity. Though proposed model has complex structure, use of SHA-1 induces its vulnerability towards collision attack [10].

B. Lossy compression and iterative reconstruction for encrypted image

In [11], authors have implemented joint image encryption and compression scheme using pseudorandom permutation for encryption and discarding excessively rough and fine

information of coefficient generated from orthogonal transform. Permutation based encryption methodologies hence used can be referred from [12] and [13]. The work permutes N pixel image so as to generate encrypted image. Encryption hence done has "N!" possible patterns. Hence it requires only brute-force to crack encrypted image hence generated. Later to compress image author has divided it into the ratio of "α" and "1-α". Author [11] have also stated system parameters **Δ**, M, where smaller **Δ** can result in a better reconstructed image since the receiver can exploit more precise information for image reconstruction, the compression ratio is determined by α and M. Different set of test results are listed for compression ratio and PSNR on Lena as test image. It has been concluded that, , since original pixel values haven't been masked in mentioned scheme hence its utility is only fixed in low confidential functionalities only.

*C. **Image encryption-compression scheme using hyper-chaos and Chinese remainder theorem***

The method to encrypt then compress or combine the image encryption and compression in single process needs to insert additional operations in the procedure and procedure is made complicated. Hence authors in [14] have used 2D hyper-chaos discrete non-linear dynamic system for encryption and Chinese remainder theorem for compression. The advantage of Hyper-chaos is, it has more than one positive Lyapunov exponents and it has complex dynamic characteristics than chaos based scheme. Proposed method is sequential application of 2D hyper-chaos discrete non-linear dynamic system and then Chinese remainder theorem. The validity of proposed scheme was tested with key space analysis, histogram analysis, correlation analysis, key sensitivity analysis, information entropy analysis, compression performance, randomness analysis, encryption quality analysis, and speed performance as comparison parameters and proposed scheme was found that, proposed scheme has comparative if not best results to pre-existing schemes. In this scheme original pixels haven't been masked, but due to double shuffling of pixels confidentiality is fairly maintained.

*D. Mo**dified JPEG (MJPEG)***

JPEG is often used for compression of digital image. The degree of compression can be selected which allows selectable tradeoff between storage size and image quality. Although it is advantageous for compression it has no provision for security. Hence, authors in [15] have aggregated GLS coding [16] and binary key stream resulting from chaotic generator based security solution with JPEG compression. It has been concluded after analyzing the result that compression performance of MJPEG was good, the key hence generated had high sensitivity and it was found immune to chosen-plaintext attack.

*E. **Joint data-hiding and compression scheme***

Compression and encryption separately are vulnerable to attacks since, compression and encryption are two separate blocks in this scheme. To reduce this vulnerability joint data-hiding and compression (JDHC) scheme has been proposed. In [17] authors have modelled JDHC scheme using Side match vector quantization (SMVQ) and image inpaniting. At senders side except leftmost and topmost blocks of the image all other blocks are encrypted and compressed in raster-scanning order. Later validity of proposed scheme was tested on Lena, Airplane, Lake, Peppers, Sailboat, and Tiffany with other three pre-existing models and it was concluded that proposed model provided at par results for data hiding, compression ratio and decompression quality with compared models. Since this scheme uses JDHC scheme it induces extra parameters in encryption and compression scheme, which increases the complexity of proposed model and since this model hasn't provided any improvement upon pretexting results its utility is limited.

*F. **Image compression-encryption scheme based on spatiotemporal cross chaotic system***

The proposed model [18] does compression then encryption by using Non-uniform Discrete Cosine Transform (NDCT) Nearest-neighbouring coupled-map lattices (NCML) [19]. Proposed scheme works by transforming image by using NDCT which utilizes CML to control non uniformity. Then quantification and Huffman coding is carried out and then permutation and diffusion are deployed to encrypt image. The proposed approach was tested on colour images and grey-scale images of Baboon, Lena and Peppers with DCT with Huffman coding and AES. It was concluded that proposed model provided two layer of security, it had large enough key to resist brute-force attack, was faster than DCT followed by AES. Proposed scheme was found to be with less distortion and good compression ratio.

*G. **Chaos based image encryption and lossless compression scheme using hash table and Chinese Remainder Theorem (CRT)***

The proposed scheme [20] uses an image encryption using chaotic maps and CRT. The plain image is divided into blocks which are scrambled using Henon maps and then Arnold cat map, then confused image is permuted using sequence from hyper chaos and hash table structure. Then image hence obtained is diffused by using Lorenz equation or matrix generated from plain image prior to compressing it using CRT. After experimental analysis it was concluded that proposed scheme provided good key space and key sensitivity hence it has good resistance to differential attacks. NPCR and UACI values were found to be completely random. Although this model had fair results, but utilizing two mapping schemes for scrambling, hash table implementation followed by CRT has produced a lengthy scheme which is taking more execution time and is slower than standard schemes.

IV. CONCLUSION

In this study it was observed that most of the methods performing encryption as well as decryption have been categorized in three categories (1) compress then encrypt (2) encrypt then compress and (3) joint data-hiding and compression scheme. Encrypt then compress scheme was found advantageous over compress then encrypt as

compression process can be performed separately in channel away from senders location so as to increase the sending speed whereas compress then encrypt has to be done at senders side only this approach slows down the transmission process. Although JDHC has provision to perform encryption and compression together and this increases the complexity of secured data. But in these processes JDHC methodologies commonly induce extra parameters which slow down transmission process. It was observed that recently chaos and hyper-chaos based encryption has been fairly popular and they can be utilized with standard encryption algorithms like affine with XOR, blowfish, twofish etc. to increase their utility in studied schemes.

V. REFERENCES

1. John Justin, M., and S. Manimurugan. "A survey on various encryption techniques." International Journal of Soft Computing and Engineering (IJSCE) ISSN 2231 (2012): 2307.
2. Yen, Jui-Cheng, and Jiun-In Guo. "A new chaotic mirror-like image encryption algorithm and its VLSI architecture." Pattern Recognition and Image Analysis (Advances in Mathematical Theory and Applications) 10.2 (2000): 236-247.
3. Sinha, Aloka, and Kehar Singh. "A technique for image encryption using digital signature." Optics communications 218.4 (2003): 229-234.
4. Maniccam, S. S., and Nikolaos G. Bourbakis. "Lossless image compression and encryption using SCAN." Pattern Recognition 34.6 (2001): 1229-1245.
5. Furht, Borko, Daniel Socek, and Ahmet M. Eskicioglu. "Fundamentals of multimedia encryption techniques." Multimedia Security Handbook 4 (2004).
6. Yuen, Ching-Hung, and Kwok-Wo Wong. "A chaos-based joint image compression and encryption scheme using DCT and SHA-1." Applied Soft Computing 11.8 (2011): 5092-5098.
7. Shi, Yun Q., and Huifang Sun. Image and video compression for multimedia engineering: Fundamentals, algorithms, and standards. CRC press, 1999.
8. Lian, Shiguo, Xi Chen, and Dengpan Ye. "Secure fractal image coding based on fractal parameter encryption." Fractals 17.02 (2009): 149-160.
9. Chen, Tzung-Her, and Chang-Sian Wu. "Compression-unimpaired batch-image encryption combining vector quantization and index compression." Information Sciences 180.9 (2010): 1690-1701.
10. Wikipedia contributors. "SHA-1." Wikipedia, The Free Encyclopedia. Wikipedia, The Free Encyclopedia, 30 Jun. 2017. Web. 5 Jul. 2017
11. Zhang, Xinpeng. "Lossy compression and iterative reconstruction for encrypted image." IEEE transactions on information forensics and security6.1 (2011): 53-58.
12. Yen, J-C., and J-I. Guo. "Efficient hierarchical chaotic image encryption algorithm and its VLSI realisation." IEE Proceedings-vision, image and signal processing 147.2 (2000): 167-175.
13. Bourbakis, N., and Christos Alexopoulos. "Picture data encryption using scan patterns." Pattern Recognition 25.6 (1992): 567-581.
14. Zhu, Hegui, Cheng Zhao, and Xiangde Zhang. "A novel image encryption–compression scheme using hyper-chaos and Chinese remainder theorem." Signal Processing: Image Communication 28.6 (2013): 670-680.
15. Zhang, Yushu, et al. "GLS coding based security solution to JPEG with the structure of aggregated compression and encryption." Communications in Nonlinear Science and Numerical Simulation 19.5 (2014): 1366-1374.
16. Luca, Mihai, et al. "A new compression method using a chaotic symbolic approach." IEEE Communications. 2004.
17. Qin, Chuan, Chin-Chen Chang, and Yi-Ping Chiu. "A novel joint data-hiding and compression scheme based on SMVQ and image inpainting." IEEE transactions on image processing 23.3 (2014): 969-978.
18. Zhang, Miao, and Xiaojun Tong. "A new algorithm of image compression and encryption based on spatiotemporal cross chaotic system." Multimedia Tools and Applications 74.24 (2015): 11255.
19. Kaneko, Kunihiko. "Spatiotemporal intermittency in coupled map lattices." Progress of Theoretical Physics 74.5 (1985): 1033-1044.
20. Brindha, M., and N. Ammasai Gounden. "A chaos based image encryption and lossless compression algorithm using hash table and Chinese Remainder Theorem." Applied Soft Computing 40 (2016): 379-390.