IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

Enhanced Compression and Cryptographic Techniques for Securing Images- A Survey

G.Elavarasi[1]*, M.Vanitha[2]

[1,2]Department of Computer Applications, Alagappa University, Karaikudi, India

Corresponding Author: elavarasig90@gmail.com,

DOI: https://doi.org/10.26438/ijcse/v7i4.344348 | Available online at: www.ijcseonline.org

Accepted: 11/Apr/2019, Published: 30/Apr/2019

Abstract- A huge amount of data has been exchanged over various types of networks due to the rapid growth of computer networks and information technology. In major part of these exchanged data, they need security mechanisms to offer various degree of protection. The common solution to protect digital data from eavesdropping and intercepting is to encrypt the message which needs some knowledge of cryptography. Cryptography is a technique used today hiding any confidential information from the attack of an intruder and used to create authentication, integrity, availability and confidentiality. Nowadays, Digital data communication requires data security, so that data should reach to the intended user in safe manner. The protection of confidential data from unauthorized access can be done with many encryption techniques. Encryption is used to protect data from being accessed by unauthorized users. It is very important to communicate images over networks. The important image transfer will takes place over the unsecured internet network. Continuing development of the various electronic image processing technologies has produced faster means of transmission. Compression is often used to save disk space and reduce the time needed to transfer images over the networks. Compressing data can save storage capacity, speed up file transfer and reduce cost for hardware storage and network bandwidth.

Keywords— *Data Compression, Data Encryption, Cryptography, Image Processing and Security Mechanism.*

I. INTRODUCTION

Cryptography plays a major role in securing data that the contents of a message are confidentially transmitted and would not be altered. The security objectives for data security are Confidentiality, Authenticity, Integrity and Non-rejection. In major part of the exchanged data, no matter whether they are confidential or private, they need security mechanisms to offer various degree of protection. The common solution to protect digital data from eavesdropping and intercepting is to either encrypt the message or encrypt the channel. Encryption is used to protect data from being accessed by unauthorized users. Many cryptography techniques are employed, such as symmetric and asymmetric techniques to provide data security. Data encryption is one of the techniques to protect information from tapping.

To transfer data, compression is used because it uses less disk space and increases the speed of data transfer. Data compression is known for reducing storage space. It involves transforming data from a specific format, called a source message to a data with a smaller format called a code word. Continuing improvement of the various electronic image-processing technologies have produced faster means of transmission, and increasingly sophisticated computer algorithms for compressing the image data have further improved both transmission speed and the quality of the transmitted images. Compression is often used to save disk space and reduce the time needed to transfer images over the networks. Data compression is a reduction in the number of bits needed to represent the data. Compressing data can save storage capacity, speed up file transfer and reduce cost for hardware storage and network bandwidth.

The objective of this paper is to analyze the existing works on cryptography which have been used for secure data from an unauthorized access during transmission. Over the past few years, various laboratories all over the world showed their intense involvement studies on Encryption and Decryption.

Section II contains the literature survey of the proposed method, Section III contains some techniques used for the present study, and Section IV concludes present study with directions for further work.

II. LITERATURE SURVEY

Chamman Lal Sahu et al. (2016) [1] discussed about jpeg encoding and compression. They proposed the analysis process of JPEG (joint picture expert group) standard which is based on the technique called discrete cosine transform (DCT). DCT is a method that converts a graphic image as jpeg from spatial domain to frequency domain. In DCT method quantization, transformation is used for removal of high frequency bit and redundancy. But when compression ratio increases, more information will be lost in DCT technique.

K. AyyappaSwamy et al. (2015) [2] proposed a new hybrid transform by combining DCT and DWT which gives better compression ratio for same PSNR. In image compression using Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) with different levels and different thresholds we can observe different compression ratio and different peak signal-to-noise ratio. When comparing DCT with DWT, results of DWT are better than DCT.

Dr.T. Karthikeyan et al. (2014) [3] discussed Embedded Zero tree Wavelet (EZW) coder and EZW algorithm. An EZW encoder is an encoder which is designed to use with wavelet transforms and also explains why it has the word wavelet in its name. The EZW coding algorithm provides outstanding compression ratio than the previous thresholding techniques by manipulating the spatial self- similarities of the zero tree structure. EZW is fully adaptive and it appears to work well with any image type.

Dr Mohammed Ismail.B (2017)[4] discussed about Fractal Image Compression (FIC) technique which has achieved intense recognition because of its desirable advantages like very high compression ratio (C.R), high decoding speed, far above the ground bit-rate, very aggressive rate distortion and non-dependency on resolution. . However, the long encoding time, complexity involved in search process and parameters of quality decoding issues are being explored by new contemporary hybrid methods in fractal coding. These new contemporary bench mark methods target to improve key issues of reduction of encoding time and maintain the fidelity of an encoded or reconstructed image.

Anita Thengade et al. (2012) [5] discussed about Genetic Algorithm and its basic functionality. The basic functionality of Genetic Algorithm includes various steps such as selection, crossover, and mutation. They focused on the comparison of Genetic Algorithm with other problem solving techniques and discussed the detailed comparison of GAs with Heuristic Search and also with other searching technique such as Simulating Annealing and Hill Climbing. It includes the various Labs that mainly concentrate on the different research that are carried out on GAs.

Peiya Li et al. (2017) [6] have proposed a new joint image compression and encryption scheme based on lossy JPEG standard, which aims at encryption power's enhancement on the premise of maintaining JPEG's compression efficiency. In the proposed scheme the secret encryption key is generated from the plain-image using BLAKE2 hash algorithm. Encryption operations include three parts: new orthogonal 8×8 transforms transformation, DC coefficients encryption, and AC encryption. Data embedding strategy is used here which reduces the cost of sending different 256-bit encryption keys to the decoder when different plain-images are compressed and encrypted.

Mohab Mostafa et al. (2017) [7] have proposed a joint image compression and encryption technique based on Compressed Sensing (CS) and Entropy Coding. Compressed sensing (CS) has been expended for compressing sparse signals. In CS it is possible to recreate a signal when only a small number of samples are available under certain conditions. Signal must be sparse and samples must be developed randomly. Five different algorithms are proposed and tested on 15 popular images.

Subhajit Roy et al. (2016) [8] apply a static HUFFMAN coding for compressing image data and apply Selective Encryption with the proposed algorithm. Selective encryption is a technique to enable new system functionality by only encrypting a portion of a compressed bit stream while security should not compromise. Selective encryption is one of the effective approaches to reduce computational cost and the possibility of frequency analysis attack is reduced. The main feature of efficient selective encryption is identification of sensitive region and process of encryption. To measure the effectiveness of the process they use Lavenshtein distance (DSID). This will evaluate the minimum number of insertion, deletion and substitution operations are required to transform source data to target data.

Prasanth P. S et al. (2013) [12] introduced a novel scheme for Lossy compression of an encrypted image. Compression is made by Discrete Cosine Transform (DCT). Image reconstructed by Inverse Discrete Cosine Transform (IDCT). Huffman coding is used for encoding. Pixel positions are shuffled and pixels values are not masked in the Encryption Phase. This system has less Security when compared to standard stream cipher. Here compress the image with wavelet compression and DCT and conclude that wavelet compression is better than DCT.

Kingston et al. (2007) [14] proposed a new joint encryption and lossless compression technique for large images. It uses the Mojette transform properties, and can easily be included in distributed storage architecture. The assessment of security performance is in terms of processing time and compression ratio. They proposed a fast selective encryption technique based on standard encryption algorithms.

Table.1 - Merits and Demerits of the Compression algorithms

S.No	Algorithms	Merits	Demerits
1	DCT(Discrete Cosine Transform)	i) It is a powerful tool for image compression. ii) The transformation is orthogonal and fast algorithms can be used for computation.	i) The input from pre-processed 8 x 8 blocks are integer-valued, the output values are typically real-valued. Thus a quantization step is needed to make some decisions about the values in each DCT block and produce output that is integer-valued.
2	DWT (Discrete Wavelet Transform)	i)The wavelet transform is well-suited for the time-frequency analysis and signal de-noising. ii) Computationally very fast. iii) It isolates the fine details in a signal. Very small wavelets can be used to separate very fine details in a signal, while very large wavelets can identify coarse details.	i) For fine analysis, it becomes computationally intensive. ii) Its discretization, the discrete wavelet transform is less efficient and natural. iii) The flexibility of DWTs is a two-edged sword which is sometimes very difficult to choose which basis to use.
3	Run Length Encoding	i)It is very easy to implement and does not require much CPU horsepower. ii) It is only efficient with files that contain lots of repetitive data. iii) Computer-generated colour images can also give fair compression ratios.	i) Not good when compare to Huffman coding.
4	Lempel-Ziv coding	i)No prior information is needed about the input data stream. ii) It can compress the input data stream in a single pass. iii) It allows fast execution.	i) It is no longer effective at compression when it reaches a certain size.
5	Vector Quantization	i) It has low computational burden when compared with other techniques such as dynamic time warping (DTW) and hidden Markov model (HMM) in Pattern recognition.	i) When compared to DTW and HMM, it does not take the temporal evolution of the signals because all the vectors are mixed up.
6	Fractal Image Compression	i) Good mathematical encoding frame. ii) High compression ratio. iii) Quick decompression. iv) High reconstruction quality at low coding rates. v) Fast decoding. vi) Resolution independence i.e.; an encoded image may be decoded at a higher resolution than the original.	i) Slow encoding. ii) Fractal image compression allows fast decoding, but encoding is very slow.
7	EZW(Embedded Zero tree Wavelet)	i) Employs progressive and embedded transmission. ii) Uses zero tree concept. iii) Uses predefined scanning order. iv) Good results without pre-stored tables, codebooks / training. v) It is possible to break the compression algorithm at any time and obtain an approximation of the original image.	i) Transmission of coefficient position is missing. ii) No real compression. iii) Followed by arithmetic encoder.
8	SPIHT(Set Partitioning in Hierarchical Trees Coding)	i) PSNR values are high for given Compression Ratios for variety of images. ii) Quad- tree or hierarchical trees are set.	i) Only implicitly locates position of significant coefficients. ii) Requires more memory. iii) Suits variety of natural images.

9	EBCOT (Embedded Block Coding with Optimized Truncation)	i) Supports packet decompositions. ii) Block based scheme. iii) Modest complexity. iv) SNR scalability can be obtained. v) Less ringing around edges. vi) Superior rendition of textures. vii) Preserves edges lost by SPIHT.	i) As layers increase, performance decreases.

Table.2 - Merits and Demerits of the Cryptographic algorithms

S.No	Algorithm	Merits	De-Merits
1	RSA (Rivest –Shamir– Adleman)	i) The use of complex mathematics is safe and secure. ii) It is hard to crash since it involves factorization of prime numbers which are difficult to factorize. iii) It uses Public Key encryption.	i) It can be very slow in cases where large data needs to be encrypted by the same computer. ii) It needs a third party to verify the reliability of public keys. Public-key cryptography is not necessary in a single-user environment.
2	DES (Data Encryption Standard)	i)Both Encryption and decryption take the same algorithm. Here, the function need to be reversed and the key must be taken in opposite order. This is very suitable for software and hardware requirements. ii) It is a 56 bit key. So there are 2^56 possibilities of keys to find the correct key.	i) Weak keys: the key is selected on the rounds are problems. During splitting of keys to two half and swapping might throw up the same result if they have continuous 1's and 0's. Thins ends up in using the same key throughout the 16-cycles. ii) Semi weak keys: same output from the S-Boxes on different inputs on permutation.
3	AES(Advanced Encryption Standard)	i) It uses 128, 192 and 256 bits keys for encryption. Hence, it makes AES algorithm more vigorous against hacking. ii) For 128 bit, about 2^{128} attempts are required to break. This makes it very tough to hack it as a result it is very safe protocol.	i) It uses too simple algebraic structure. ii) Each and every block is always encrypted in the same way. iii) Hard to implement with software. iv) AES in counter mode is difficult to implement in software taking both performance and security into considerations.
4	Blowfish	i) It is one of the fastest block ciphers in general use, except when changing keys. ii) It does not subject to any patents. Therefore it is freely available for anyone to use.	i) Each pair of users' needs to be unique, so as number of the users increase, key management becomes complicated. ii) It can't provide Authentication as well as non-repudiation as two people have the same key. iii) In decryption process, it has the weakness in terms of time consumption and serially in throughput.
5	Message Digest 5 (MD5)	i) MD5 is much easier to implement as compared to other hash functions. ii) The MD5 algorithm is not limited to multiples of eight bit (octets, bytes). iii) It stated for messages consisting of any number of bits.	i) One of the basic requirements of hash function is that it should be computationally infeasible to find two distinct messages which hash to the same value. MD5 fails this requirement. ii) Not all approaches to obtain MAC (Message Authentication Code) through MD5 are attack resistant.
6	Secure Hashing 1 (SHA 1)	i) SHA-1 is easy to implement as compared to a few other hashing algorithms. ii) SHA-1 is easily available and it provides good resistance against attacks. iii) It is more secure than MD5. iv) It is less likely to have collisions in case of SHA-1.	i) SHA-1 is more complex to implement than MD5.

III. CONCLUSION

This survey discussed about data compression and cryptographic algorithms. Both of these algorithms have their respective goals; the purpose of data compression is to reduce file size, while the purpose of cryptography is to secure a file in order to avoid data leakage. There are various terminologies discussed which are used for different purposes depending on the type of data used. But this paper only discusses the general idea about the Compression techniques such as EZW, JPEG, DCT, DWT, Fractal compression, Vector Quantization, Huffman coding and the Cryptographic techniques such as Genetic Algorithm, RSA, AES, DES, Blowfish, MD5, SHA-1. Each technique has some disadvantages like implementation difficulty, complexity, slow when using large data, etc... Thus

considerable research effort is still essential for secured communication.

IV. ACKNOWLEDGEMENT

This research work has been supported by RUSA PHASE 2.0, Alagappa University, Karaikudi.

REFERENCES

[1] Chamman Lal Sahu , Chandra Shekhar Singh Thakur , Manoj Kumar Xalxo , Mohit Thakur , Miss RoshniRathour, "Survey on JPEG Image Compression Using DCT", Volume 4 Issue X, October 2016, International Journal for Research in Applied Science & Engineering Technology (IJRASET).

[2] K. AyyappaSwamy , C. Somasundar Reddy, K. DurgaSreenivas , "Image Compression Using Hybrid DCT-DWT Transform", International Journal of Advanced Research in Computer Science and Software Engineering 5(5), May- 2015.

[3] Dr.T. Karthikeyan, C. Thirumoorthi, "A Survey on Embedded Zero Tree Wavelet ", 2014 International Journal of Computer Science.

[4] Dr Mohammed Ismail.B, "Contemporary Bench Mark Techniques in Fractal image Compression-A Survey", International Journal of Engineering Technology Science and Research IJETSR, October 2017.

[5] Anita Thengade, RuchaDondal, "Genetic Algorithm – Survey Paper", International Journal of Computer Applications, April-2012.

[6] Peiya Li, Kwok-Tung Lo, "A Content-Adaptive Joint Image Compression and Encryption Scheme", 1520-9210 (c) 2017 IEEE

[7] Mohab Mostafa L, Mohamed Waleed Fakhr, "Joint Image Compression and Encryption Based on Compressed Sensing and Entropy Coding", 2017 IEEE 13th International Colloquium on Signal Processing & its Applications (CSPA 2017), Penang, Malaysia

[8] Subhajit Roy, Prof.(Dr.)GautamSanyal, "An Approach to Selective Encryption on Compressed Image ", on 2016 2nd International Conference on Contemporary Computing and Informatics (ic3i)

[9] Kalyani G. Nimbokar, Milind V.Sarode, MangeshM.Ghonge, "A Survey based on Designing an Efficient Image Encryption-then-Compression System", International Journal of Computer Applications (0975 – 8887) National Level Technical Conference "X-PLORE 14

[10] Ganesh Lamkhade, Ajay Kumar Gupta, "A Survey on Efficient ETC (EncryptionThenCompression) Techniques for Image Data Security", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Impact Factor (2012): 3.358

[11] Maria Joseph, Tomson Devis,"Highly Secure Scalable Compression of Encrypted Images", IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308, Oct -2015

[12] Prasanth P. S, Anusree L, "Lossy Compression and Reconstruction for Encrypted Image", International Journal of Computer Science and Mobile Computing, ICMIC13, December-2013, pg. 153-157

[13] G. Elavarasi, Dr. M. Vanitha, "A Novel Method for Securing Medical Image Using Visual Secret Sharing Scheme", International Journal of Engineering and Technology (IJET), Vol 9 No 5 Oct-Nov 2017

[14] A. Kingston, S. Colosimo, P. Campisi, F. Autrusseau," Lossless Image Compression and Selective Encryption Using a Discrete Radon Transform", 2007 IEEE

[15]Abraham Jun Jiang Lock, Chong HooiLoh, SitiHasanahJuhari, AzmanSamsudin, "Compression-Encryption Based on Fractal Geometric", Second International Conference on Computer Research and Development, 2010 IEEE

[16] Xinpeng Zhang, "Lossy Compression and Iterative Reconstruction for Encrypted Image", IEEE Transactions on Information Forensics and Security, VOL. 6, NO. 1, MARCH 2011

[17] Subhajit Roy , Prof.(Dr.)GautamSanyal, "An Approach to Selective Encryption on Compressed Image ", 2016 2nd International Conference on Contemporary Computing and Informatics (ic3i), IEEE

[18] Daniel Schonberg, Stark Draper, Kannan Ramchandran, "On Compression Of Encrypted Images", UC Berkeley, EECS Department, 211 Cory Hall #1772, Berkeley, CA 94720-1772 {dschonbe,sdraper,kannanr}

[19] B.Suneetha, "Designing an Efficient Image Encryption-then Compression System", International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering Vol. 3, Issue 3, March 2015

[20] EmySetyaningsih, RetantyoWardoyo, "Review of Image Compression and Encryption Techniques", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 2, 2017

[21] Xinpeng Zhang, Member, IEEE, Yanli Ren, Liquan Shen, Zhenxing Qian, and GuoruiFeng, "Compressing Encrypted Images With Auxiliary Information", IEEE Transactions On Multimedia, VOL. 16, NO. 5, AUGUST 2014

[22] S. Dubey, R. Jhaggar , R. Verma and D. Gaur, "Encryption and Decryption of Data by Genetic Algorithm", International Journal of Scientific Research in Computer Science and Engineering Vol.5, Issue.3, pp.42-46, June (2017)

[23] V. Kapoor, "A New Cryptography Algorithm with an Integrated Scheme to Improve Data Security", International Journal of Scientific Research in Network Security and Communication, Volume-1, Issue-2, June- 2013

