[NC-Rase 18]
DOI: 10.5281/zenodo.1485342

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

A NOVEL APPROACH TOWARDS PROVIDING SECURITY TO THE IMAGES BY USING COMPRESSION AND ENCRYPTION MECHANISM

Kiran H. Ghate[1], Kalyani S. Hatwar[2], Sayali M. Jawake[3] & Kranti Bhoyar[4]
[1,2,3]Assi.Prof. Computer Science and Engg. Department, MGICOET, Shegaon
[4]Assi.Prof. Electronics and Telecommunication Department, MGICOET, Shegaon , Maharashtra, India

ABSTRACT

Data compression is used for reducing storage in network as well memory and communication costs. It involves transforming data of a given format, called source message to data of a smaller size format called code word. Data encryption is for protecting formation from eavesdropping. It transforms data or image content of a given format, called plaintext to another format called cipher text, using an encryption method with the help of key. The major problem existing with the current compression and encryption method is the speed, the processing time required by a computer. To lessen the problem, combine the two processes into one process which takes less time compare to performing both the processes separately. The data will be first compressed using compression algorithm and then encrypted using AES algorithm and then comparative analysis will be carried out for different combinations of compression and encryption techniques. More notably, the proposed encryption technique applied to compressed images is good in compression efficiency. If encryption and compression are done at the same time then it takes less processing time and more speed as compare to existing one.

Keywords*: Image Compression, Image Encryption, Huffman algorithm, LZ77 algorithm, AES.*

I. INTRODUCTION

Security of network communication is arguably the most important issue in the world today given the vast amount of valuable information that is passed around in various networks. While larger files sent on network with security, it has to be encrypted. The files larger in size when encrypted still increase in size. Hence normally it's compressed and sent across the network. Data compression is generaly used for reducing storage and communication costs. It involves transforming data of a given format called plaintext, to another format called cipher text, using an encryption key [1].

The security of multimedia software products become more important, since multimedia data are transmitted over open network more frequently [2]. Typically, security is necessary to content protection of digital images and videos. Encryption schemes used for multimedia data need to be specifically designed to protect multimedia content and fulfill the security requirements for a particular multimedia application. For example, real time encryption of an image using classical ciphers requires heavy computation due to the large amounts of data involved, but many multimedia applications requires security on a much lower level, this can be achieved using selective encryption that leaves some perceptual information after encryption [3].

Due to the fast progression of data exchange in electronic way, information security is becoming more important in transmission. It must to protect the confidential image, video and textual data from unauthorized access. The data security is done by two techniques one is cryptography other is steganography. Proposed method use cryptography. Cryptography I the science of protecting data, which provides methods of converting data into unreadable form, so that valid user can access information at the destination. Cryptography is the mechanism of using mathematics to encrypt and decrypt data [4]. Figure 1.1 shows cryptographic process in which P represent plaintext, C represent cipher text stands for encryption and D stand s for decryption .A marked progress built in the field of images.

[NC-Rase 18]
DOI: 10.5281/zenodo.1485342
ISSN 2348 – 8034
Impact Factor- 5.070

II. LITERATURE REVIEW

There are four techniques for compression, discrete cosine transform (DCT), vector quantization (VQ), fractal compression, and discrete wavelet transform (DWT). Discrete cosine transform is algorithm which is a lossy compression that samples an image at regular intervals, analyzes the frequency components present in the sample, and discards those frequencies which don't affect the image as the human eye realize or understands it. DCT is the basis of standards such as JPEG, BMP, MPEG, H.261 and H.263. Vector quantization is a lossy compression method that looks at array of data, an alternative of individual values. It can then generalize what it sees, compressing superfluous or redundantdata, while at the same time retaining the desired object or data stream's original intent. Fractal compression is a form of VQ and is also one of the lossy compression technique which is used. Compression is performed by locating self-similar or correlative sections of an image, then using a fractal algorithm to generate the sections. Like DCT, discrete wavelet transform ,transforms an image into frequency components mathematically. The process performed on the image, which differs from the other methods (DCT) that work on smaller pieces of the desired data. The result is a hierarchical representation of an image, where each layer represents a frequency band [24].

Cryptanalysis is art of breaking cryptosystems, seeing through the disguise even when you're not supposed to be able to. Cryptology is about both cryptography and cryptanalysis. Today's cryptosystems are divided into two categories: symmetric and asymmetric. In Symmetric cryptography the same key used to encrypt and decrypt a message, and asymmetric cryptosystems use one key to encrypt a message and a different key to decrypt it and all of today's algorithms fit within those two categories. Asymmetric cryptosystems are also called public key cryptosystems. We have shown that the field of Cryptography has evolved tremendously since the Assyrian and Egyptian time, and as the technology progresses and computers become faster and advanced, it will be easier to cultivate the power of distributed processing and break the different encryption algorithms such DES or triple DES, thus Cryptology is an evolving field [25].

According to [6] there are three basic methods of secured communication available, namely, cryptography, steganography and watermarking. Among these three, the first one, cryptography, deals with the development of techniques for converting information between comprehensible and incomprehensible forms during information exchange. Steganography [7][8], on the other hand, is a technique for hiding and extracting information to be conveyed using a carrier signal. The third one, watermarking [9][1.0], is a means of developing proper techniques for hiding proprietary information in the perceptual data. For the compression [11][12] of image mainly two types of techniques are used Lossless compression techniques and Lossy compression techniques. Name itself indicates the lossless compressions will not going to introduce any noise to the original image and thus the decompression techniques had been used by them to reduce the redundancy. Howard Cheng and Xiaobo Li [13] performed compression using quad tree compression algorithm. And only partial encryption is applied. 13-27% of the output from quad tree compression algorithms and less than 2% for 512X 512 images compressed by the SPIHT algorithm is encrypted. Limitation is that a different scheme has to be designed and analyzed for each compression algorithm. A. Alfalou C. Brosseau et al. [14] performed compression based on the discrete cosine transform (DCT). Two levels of encryption are used. The first one is grouping of the DCTs in the spectral domain and second transformation, i.e. to hide the transmitting images, one of the input images is used as encryption key. The compression is better te.avt!,,,41 -4) t-4 otc(f-ofiv than JPEG in terms of PSNK. The proposed mechanism achieves PSNR as 21.7186 as compared to that of JPEG as 20.6904 on applying on Lena image. N.V.Thakur and O.G.Kakde [15] proposed the decompression and encryption based on the fractal coding and spiral architecture but the compression method are lossy. To reduce time complexity of fractal coding FFT based cross correlation is used. Any certain encryption method is not specified and any stream cipher algorithm can be used. Their experimental results are better than quadtree method w.r.t. PSNR ratio and encoding time. Mingyu Li et al. [16] used a RC5 stream cipher based scalable encryption scheme for low complexity transparent transcoding. CCSDS compression technique is used which consist of two part DWT and Bit plane coding. Advantage is that Encryption is scalable. V.Radha, D.Maheswari [17] proposed image encryption algorithm that consists of two parts: scrambling of plain-image and mixing operation of scrambled image using discrete states variables of chaotic maps. Discrete Cosine transform is, used for compression. The proposed algorithm is strongly provide security and is also very fast. Since the key space

is large therefore the attacker cannot decrypt an encrypted image without the correct key. Alfalou et al. [18] used DCT to jointly compress and encrypt the image with a new system able to amalgamate spectral information. That fusion allows the compression and the encryption of information at the same time. Authors also specify that it is possible to use the DCT to jointly realize a compression and an encryption of the data by spectral fusion thus allowing a very important gain in transmission time. Shiguo Lian et a/. [19] proposed a totally different scheme. They carried out encryption before and after compression. JPEG is used for image compression. Using chaotic stream cipher encryption is carried out. Encyption consists of three parts: color plane Confusion, Sign encryption and DCT coefficient confusion space. They achieved the 75% compression ratio and 7.6%Encryption time ratio on Lena image of size 256x256.Kumar and Makur applied the approach to the prediction error domain and achieved better lossless compression performance on the encrypted grayscale/color images [20]. Aided by rate-compatible punctured turbo codes, Liu et. al developed a progressive method to losslessly compress stream cipher encrypted grayscale/color images [20]. Klinc et al. extended Johnson's framework of compressing block cipher encrypted data. To achieve high compression ratios, lossy compression of encrypted data was also studied. Zhang et. Al proposed a scalable lossy coding framework of encrypted images via a multi-resolution construction [12]. A compressive sensing (CS) technique was utilized to compress encrypted images resulted from linear encryption. A modified basis pursuit algorithm can be applied to estimate the original image from the compressed and encrypted data. Another CS-based approach for encrypting compressed images was reported [20].Zhang designed an image encryption scheme via pixel-domain permutation, and demonstrated that the encrypted file can be efficiently compressed by discarding the excessively rough and fine information of coefficients in the transform domain [12].Zhang et. al suggested a new compression approach for encrypted images through multi-layer decomposition [21]. This paper basically provides a survey of different basic lossless data compression algorithms. Experimental outputs or resulys and comparisons of the lossless compression algorithms using Statistical compression techniques and Dictionary based compression techniques were performed on text data. Among the statistical coding mechanism the algorithms such as Shannon-Fano Coding, Huffman coding, Adaptive Huffman coding, Run Length Encoding and Arithmetic coding are considered. Lempel Ziv scheme which is a dictionary based technique is divided into two families: those derived from LZ77 (LZ77, LZSS, LZH and LZB) and those derived from LZ78 (LZ78, LZW and LZFG). A set of interesting conclusions are derived on their basis. Lossy algorithms achieve better compression as well effectiveness than lossless algorithms, but lossy compression is limited to audio, images, and video, where some loss is acceptable. The question of the better technique of the t‘ko, lossless- or lossy- is pointless as each has its own uses with lossless techniques better in some cases and lossy technique better in others [5].

III. SYSTEM DESIGN

The basic idea behind the present work is to select the part of the image by the arranging the bit stream in grid form and choosing the diagonal of the grid. Presented novel approach to providing security to images by using compression and encryption mechanism, the first one encrypts the image. In order to improve the security level we are using AES encryption algorithm with key size 128 bit which will perform at the sender side. For compression of image, we are using a Gzip algorithm can be exploited to efficiently compress the images. Al the receiving end, the receiver will sequentially perform the decompression of the image and decryption to get reconstructed image. The idea behind this method is to reducing the size of repeating string of characters. If data have more than two consecutive characters then this method would give better result. An image is actually a 2-Dsignal processed by human visual system [22]. Image can be both analog and digital type . however, at the time of process, storage [22], me of process and transmission it has to be in the form of digital type. A digital image is nothing but a 2- D array of pixels. Image plays a key role in part of providing inform significantly in remote sensing, medical specialty and video conferencing applications.

Image Compression: Image compression is the way of reducing the amount of information needed to represent a digital image. Compression is performed by reducing one or a lot of the 3 basic data redundancies:

i. Coding Redundancy
ii. Interpixel Redundancy
iii. Psychvisual Redundancy

Coding redundancy is present once when optimum code words are used. Interpixel redundancy is obtained from correlations between the pixels of a picture.psychovisual redundancy refers to those information that's unrecognizable by the human visual system (i.e. visually non-essential information). Image compression techniques decreases the amount of bits required to represent an image by taking advantage of those redundancies. An inverse method known as decompression (decoding) is applied to the compressed image to obtain the reconstructed image.

Image Encryption: Encryption and decryption are two phases of a process called cryptography [22], [23]. Cryptography is a process of storing •and transmitting data in a form that only intended person can read and process it. It is a science of protrecting information bY encoding it into an unreadable format. Data that can be read or understood without any special measurement is called plaintext

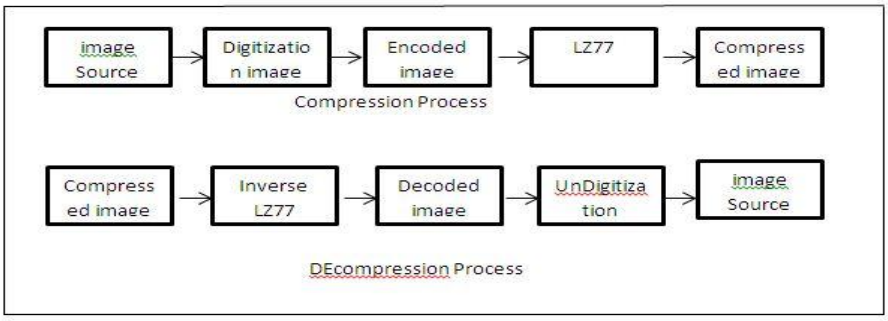

Figure 1: Basic compression

The method of rearranging the data into some unreadable form is called encryption. Encrypted plaintext is called cipher text. The algorithm used to encrypt a plaintext is called cypher. An algorithm works in a combination with a key — a word, number, or phrase — to encrypt the data. Here in case of image encryption symmetric key algorithm has been used.

System architecture

Data compression is known for reducing storage and communication costs. It involves transforming data of a given format, called source message to data of a smaller sized format called code word. Data encryption is known for protecting information from eavesdropping. It transforms data of a given format, calledcipher text, using an encryption key. The major problem existing with the current compression and encryption method is the speed, i.e. the processing time required by a computer. To lessen the problem, combine the two process into one.

Working

Compression and encryption methods are done separately the major Problem existing with the current compression and encryption methods the speed, i.e. the processing time required by a computer. Because doing two processes takes more time. To lessen the problem, this approach combines the two processes into one .i.e. proposed a new approach which will perform both encryption and compression at the same time. This approach lessons the processing time required by a computer to do the compression and encryption processes. Data compression is often referred to as coding, where coding is a very general term encompassing any special representation of data which satisfies a given need. A simple characterization of data compression is that it involves transforming a string of character in some representation into a new string which contains the same information but whose length is as small as possible.

Gzip Compression Algorithm

Gzip algorithm is made up of DEFLATE algorithm which is combination of two compression algorithms that is Huffman coding, and LZ77 compression. LZ77 is an algorithm designed to compress repeated sequences of characters, for example you scan replace "internee with a pair pointing to the offset where that sequence appeared before and the length of it. In LZ77 you use a bit to distinguish literal characters from repetitions (pairs). There are a zillion (really) variants of LZ77 but they all revolve around the same idea. Huffman codes areaway to construct a

[NC-Rase 18] ISSN 2348 – 8034
DOI: 10.5281/zenodo.1485342 Impact Factor- 5.070

code for a character based on its frequency. originally any "byte" from your input file uses 8 bits, via Huffman you create a code where the most frequent bytes will be represented in less than 8 bits and the not so frequent bytes can take more than bits.

LZ77 Compression Algorithm

LZ77 algorithms achieve compression by replacing repeated occurrences of data with references to a single copy of that data existing earlier in the uncompressed data stream. A match is encoded by a pair of numbers called a length distance pair, which is equivalent to the statement "each of the next length characters is equal to the characters exactly distance characters behind it in the uncompressed stream", (the distance " is sometimes called the "offset" instead.)To spot matches, the encoder must keep track of some amount of the mom recent data, such as the last 2 kB, 4 KB, or 32 kB. The structure in which this data held is called a sliding which is why 1277 is sometimes called Ailing window compression, The encoder needs to keep this data to 1ook for matches, and the decoder needs to keep this data to interpret the matches the encoder refers to, The larger the sliding window is, the longer back the encoder may search for creating references.

For example you might find that "e" is encoded OS "0 1" in binary taking, only 2 bits while "}" is encoded as 001010100010 taking 12 bits, Now imagine you represent the lengths of your LZ77 pairs as extra characters, you will have 256+n characters then. You build a Huffman tree from that and you have a way to encode characters and lengths with the same codes. So "01" might be "e", 001010100010 might be "}" and 00010010011101 might be "length 4". Now when you compress your file at each point you might output either a character or a repetition. If' a character you just output its Huffman code from your Huffman table. If a repetition you output the length from your Huffman codes table and then you follow with the offset.

Huffman Compression algorithm

Huffman's patent has long since expired and no license is required. There are however many variations of this method still being patented. The code can easily be implemented in very high speed compression systems. The Huffman code assumes "prior knowledge" of the relative character frequencies stored in a table or library, A secret table made available only to authorized users can be used for data encryption. A more sophisticated and efficient lossless compression technique is known as "Huffman coding", in which the characters in a data file are converted to a binary code, where the most common characters in the file have the shortest binary codes, and the least common have the longest. The Huffman Compression algorithm is an algorithm used to compress files. It does this by assigning smaller codes to frequently used characters and longer codes for characters that are less frequently used. Huffman Compression, also known as Huffman Encoding, is one of many Compression techniques in use today. Others are LZW, Arithmetic Encoding, RLE and many more. one of the main benefits of Huffman Compression is how easy it is to understand and implement yet still gets a decent compression ratio on average files. Example: the Huffman tree is i as shown below

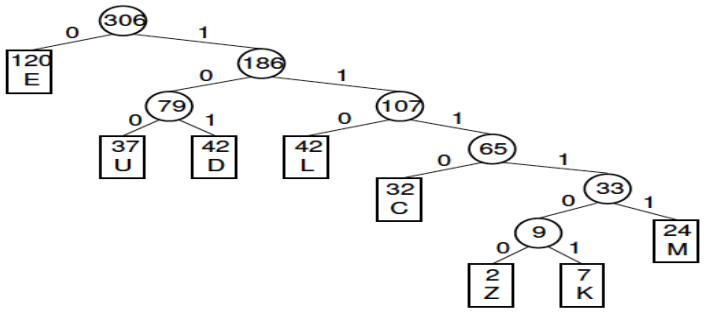

Figure 2: Huffman tree

Each non leaf node of the tree has two child nodes, the left child node and the right child node. The non-leaf node is known as the parent node of these two child nodes. Similarly the parent of a parent node is the grandparent of the child nodes. The parent, grand parent, great grandparent etc. are collectively called the ancestors of a child node.

ISSN 2348 – 8034
Impact Factor- 5.070

The child nodes are called the descendants of the ancestors. In the tree above node 3 is the parent of nodes 6 and 7. Node 1 is the parent of 3. It is also the grandparent of nodes 6 and 7. Generally nodes 3 and 1 are the ancestors of nodes 6 and 7. Nodes 6 and 7 are the descendants of nodes 3 and 1. Note that if n characters are present in a file then the number of nodes in the Huffman is 2n-1. If there are n nodes in a tree then there can be at most (n+1)/2 levels, and at least log2(n+1) levels. The number of levels in a Huffman tree indicates the maximum length of code required to represent a character.

AES Encryption algorithm

AES (acronym of Advanced Encryption Standard) is a symmetric encryption algorithm.The algorithm was developed by two Belgian cryptographers Joan Demen and Vincent Rijmen. AES was designed to be efficient in both hardware and software and supports a block length of 128bits. In proposed system we are using AES with key size of 128, 192, and 256 bits. In proposed system we are using AES with key size of 128 bits, the the following figure shows the process of AES algorithm

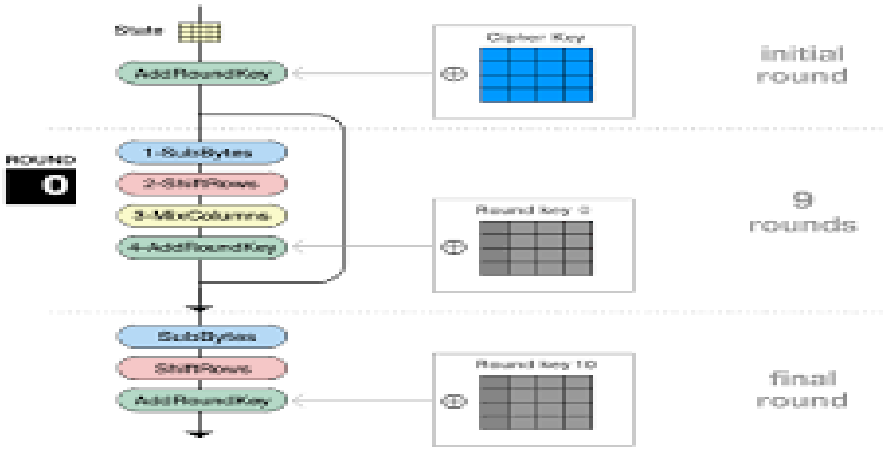

Figure 3: Working of AES algorithm for 128 hit key size

Compression and Encryption Mechanism

Working Methodology:

AES Algorithm steps:

1. Key Expansions—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.
2. Initial Round
1. Add Round Key—each byte of the state is combined with a block of the round key using bitwise xor.
3. Rounds

Sub bytes- a non-linear substitution step where each byte is replaced with another according to a lookup table.

Shift Rows- a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

Mix Columns- a mixing operation which operates on the columns of the state, combining the four bytes in each column.Add Round Key

4. Final Round (No Mix Columns)

Sub Bytes, Shift Rows, Add Round Key.

ISSN 2348 – 8034
Impact Factor- 5.070

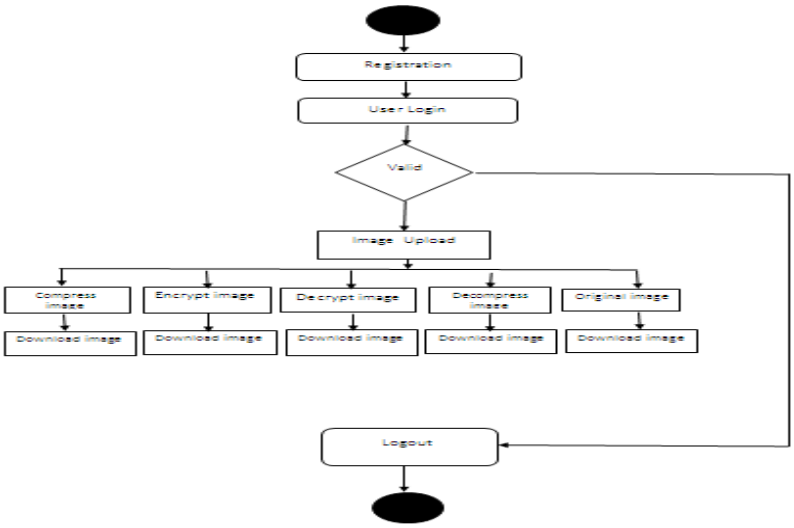

Figure 4: Data Flow Diagram of Compression and Encryption Mechanism

IV. RESULT

If encryption and compression are done at the same time then it takes less processing time and more speed. Problem Definition Currently compression and encryption methods are done separately. The major problem existing with the current compression and encryption methods is the speed, i.e. the processing time required by a computer .Because doing two processes takes more time. To lessen the problem, our approach combines the two processes (Compression and Encryption) into one process. In the new approach both encryption and compression are done at the same time. It takes less processing time and more speed. For compression Gzip compression algorithm is used. For encryption AES 128 bit algorithm is used. After encryption we will get encrypted image in compressed domain and hence not identical to original image .Finally this folder is send across the network. Once encrypted no other than the intended it hence compression and encryption is done simultaneously. After applying the combination of Compression and encryption following result will be carried out. Here we take three different gray scale images with different file format which are different in size eline.jpg, daneing.bmp and lena.png.

Table 1. Comparision between BTC, DCT and LZ77 & Huffman

File Name	Original size	Compressed file using BTC	Compressed file using DCT	Compressed file using LZ77 and Huffman
Eline.jpg	120KB (1,23,055bytes)	121KB	120KB (1,23,040 bytes)	119 KB (1,22,314bytes)
Dancing.bmp	163KB (1,67,578bytes)	163KB	154KB (1,54,500bytes)	98.7KB (1,01,165bytes)
Lena.png	295KB (3,02,807bytes)	296KB	290KB (3,02,807bytes)	289KB (2,96,032bytes)

V. FUTURE SCOPE

This product is limited to compression then encryption of single image. Research can extend to work on the different images simultaneously. May in future more improvements or facilities like by enhancing the number of pixels quality can be considered. Research can also extend this work for the infinite number of users. it can be also possible

[NC-Rase 18] ISSN 2348 – 8034
DOI: 10.5281/zenodo.1485342 Impact Factor- 5.070

to apply new formulas or algorithm for the enhancement of compression ratio in compressing of images and reducing time for execution. The proposed algorithm can be implemented on different tools also.

VI. CONCLUSION

Besides the obvious execution time advantages of combining the two processes of data compression and encryption, the encryption strength of proposed methods are as good as any other encryption algorithms such as DES, triple DES, and RC5. In this approach the speed is high because here system needs to encrypt the compressed file rather than the original file. The encryption strength is depending on the encryption key. This approach mainly developed to reduce storage requirement, improve the speed and provide the security. It has many advantages of doing this; it can transfer more and more data via internet. If combination is used it may be less costly, more secureThis fragment should obviously state the foremost conclusions of the exploration and give a coherent explanation of their significance and consequence.

REFERENCES

1. *SuhhamastanRao. M.Soujanya, T.Hemaiatha, T.Revathi, "Simultaneous data compression and encryption", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2, May 2011, ISSN M-5-4646, pp. 551-556.*
2. *R. Mehala and K. Kuppusamy, "A New Image Compression Algorithm using Haar Wavelet Transformation", International Journal of Computer Applications(0975-8887), International Conference on Computing and information Technology, November 2013, pp. 34-36.*
3. *Jiantao Zhou, Xianming Liu, Oscar C. Au and Yuan Yan Tang, "Designing an Efficient Image Encryption-Then-Compression System via Prediction Error Clustering and Random Permutation", IEEE Trans. Inf. Forensics security Vol. 9, issue 1, January 2014, pp. 85-90.*
4. *Ms. Ayushi Aggrawal, Anju, "Enciphering Data for Large Files", International Journal Of Advance Research In Computer Science And Software Engineering, Vol. 3, Issue %, May 2013, ISSN: 2277 128X, pp. 70-89.*
5. *R. Lourdusamy, "A Comparative Study of Text Compression Algorithms", International Journal of Wisdom Based Computing, Vol.1, December 2011, pp. 54-55.*
6. *A. Mitra, Y V Subbarao and S.R.M Prasnna, "A New Image Encryption approach using combination permutation technique", journal of computer science, Vol.1 No1,july2006,pp.127-133*
7. *J. Elbert and C. Paar, "An Instruction-Level Distributed Processor for Symmetric-Key Cryptography.'" IEEE Trans. Parallel and distributed systems. Vol. 16. no. 5, May 2005, pp. 468-480.*
8. *W. Stallings, -Cryptography and network security" .Englewood Cliffs, NJ Prentice Hall, 2003.*
9. *E. Besdok Hiding information in multispectral spatial image", Int.J Electron, Commun.(AEL.. 2005.. pp. 15-24.*
10. *S. Trivedi and R. Caul "Secret key Estimation In Sequential Steganography"-. IEEE trans. Signal Processing, Vol. 53, February2005, pp. 235-247.*
11. *Subrarnanya A,"Image Compression Technique" Potentials IEEE. Vol. 20, Issue 1. Feb-March 2001,pp.. 19-23.*
12. *David Jeff Jackson & Sidney Joel Hannah,"*
Comparative Analysis of image Compression Techniques,- System Theory- 1993. Proceedings SSST '93, 25th Southeastern Symposium, 7-9 March 1991 pp. 513-517.
13. *Howard Cheng and Xiaobo Li, "Partial Encryption of Compressed Image and Videos", IEEE Transactions On Signal Processing . Vol. 48. No_ S. August 2000, pp. 2439-2451.*
14. *A. Alfalou C. Brosseau. N. Abdallah_ and M. Jridi -Simultaneous fusion. compression, and encryption of multiple images-. OPTICS LAPRESS 24024, Vol. 19, No. 24 OSA, December 2011. Pp.206-210.*
15. *N. V. Thakur, and 0. G. Kakde_ -Compression Mechanism for Multimedia System in consideration of Information Security,"Proceeding International workshop on Machine intelligence Research MIR Day GHRCE-Nagpur, India, August 2009. pp. 87-97.*
16. *j. Mingyu Li. Xiaowei Yi and fienetai Ma. "A Scalable Encryption Scheme for CCSDS Image Data Compression Standard- 978-1-4244-6943-7/IEEE. April 2010, pp. 646-649.*
17. *V. Radha, D. Maheswari, "Secured Compound Image Compression Using Encryption Techniques", 978-1-4244- 5967-4/ IEEE, 2010, pp. 54-77.*

ISSN 2348 – 8034
Impact Factor- 5.070

18. *A. Alfalou, A. Loussert, A. Alkholidi, R. El Sawda, "System for image compression and encryption by spectrum fusion in order to optimize image transmission ", ISEN-BREST Laboratoty L@BISE1V, France, IEEE, 2007.*
19. *Shiguo Lian, Jinsheng Sun, Zhiquan Wang, "A Novel Image Encryption Scheme Based-on JPEG Encoding", Proceedings of the Eighth International Conference on Information Visualisation (IV'04) 1093- 9547/IEEE, 2004, pp. 556.*
20. *Cinu Joseph et al, "A Survey of Encryption then Compression using Auxiliary Information" IJCSET(www.ijcset.net)Vol6,Issue1,January2016,pp.238-240.*
21. *Shuqun Zhang and Mohammed A.Karim, "Color image encryption using double random phase encoding", Microwave and Optical Technology Letters Vol. 21, No. 5, June 5 1999, pp. 318-322.*
22. *Rafael C. Gonzalez, Richard E. Woods, Steven L. Eddins,"Digital image processing using MATLAB", December 26, June 2003.*
23. *Ross Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems", 2nd edition, March 2001, pp. 89-91.*
24. *Navpreet Saroya, Prabhpreet Kaur, "Analysis of IMAGE COMPRESSION Algorithm Using DCT and DWT Transforms", Vol. 4, Issue 2, February 2014, pp. 89-96.*
25. *Cipher A. Deavours and Louis Kruh, "Machine Cryptography and Modern Cryptanalysis", Artech House, 1985.*