A Study of Image Compression and SHA 256 Encryption Algorithms for Secure Transmission

S. Gopinathan
Dept. of Computer Science
University of Madras
Chennai, India

M. Suganthi Vinoj
Dept. of Computer Science
University of Madras
Chennai, India

ABSTRACT
This paper proposed an integrated image compression and encryption technique using similiar to color cell compression techniques with Secure Hash Algorithm 256 .The purpose of image compression is to represent images with less data in order to save storage costs or transmission time with secure. Digital images, which covers the high percentage of the multimedia data, its protection is very important. It designed a lossy compression that exploits the pixel redundancy and visual imperceptibility of human eye to fine details in the digital image. This can be achieved by image Compression process, to reduce the pixel and visual redundancy, adjacent pixels can be used to only stores RGB colour information in each pixel continuously .For encryption ,using secure hash functions the bit length of the digest they produce 256 bit message for the purpose of security for transmitting digital image.

Keywords
Image compression. secure hash algorithm, encryption

1. INTRODUCTION
Digital images, which covers the high percentage of the multimedia data, its protection is very important. To ensure the security of digital data while transferring through networks, cryptographic techniques are used. Image encryption is one of them , it provides a high level security to the image. Larger images are difficult to process hence image compression can be done after encryption process. To prevent data loss during transmission and to promote faster transmission, many different compression algorithms are used to reduce the size of the data during transmission.

2. RELATED WORK
[1] The image is all insecure for use in applications of image not secure in wireless communication. As a remedy, his paper security enhancements and an enhanced cryptosystem is proposed to make it completely resistive against above and other types of cryptanalytic attacks and increase on its plain image sensitivity and statistical encryption strength [Musheer Ahmad , M.N. Doja , M.M. Sufyan Beg b 2018][2]The main idea of the algorithm is to use one half of image data for encryption of the other half of the image reciprocally. Distinct characteristics of the algorithm are high security, high sensitivity and high speed that can be applied for encryption of gray-level and color images. The first does pre-processing operation to shuffle one half of image. The second uses hash function to generate a random number mask [Seyed Mohammad Seyedzade, Reza Ebrahimi Atani, Sattar Mirzakuchaki,2010].[3] Advanced discrete cosine transform (ADCT) based coder potentially provides a good compromise between CR and image quality but consumes essential resources for reaching a desired quality of compressed data. This approach performs sufficiently faster than compression and allows saving time and resources. It is shown that if an image to be compressed is corrupted by noise, prediction correction is possible and desirable. [Sergey Krivenko1, Mikhail Zriakhov1, Vladimir Lukin1,Benoit Vozel2,2018]. [4] The random matrix of the discrete fractional random transform is controlled by a chaotic sequence originated from the high dimensional hyper-chaotic system. Then the compressed spectrum is encrypted by the discrete fractional random transform. The order of DFrRT and the parameters of the hyper-chaotic system are the main keys of this image compression and encryption algorithm.[Lihua Gong a,b,c , Chengzhi Deng a , Shumin Pan b , Nanrun Zhou b,2018]. [5]The security implications are investigated by considering brute force and structured attacks. Robustness is characterized empirically. the CS based encryption is found to have fair robustness against additive noise, making it a promising "robust encryption" technique for multimedia. [Adem Orsdemir, H. Oktay Altun, Gaurav Sharma, Mark F. Bocko,2009].[6] The three encrypted andcompressed color components' dimensions are smaller than the original image, thus they can be grouped into a gray image, and then the gray image is scrambled by Arnoldtransform to enhance the security[Aidi Zhang1, Nanrun Zhou1,2,2013].[7] Dimensional reduction and random projection, to compress and encrypt a digital image at same time block Arnold scrambling is used to solve the position of measurements. Bitwise XOR operation is executed on binary bit stream to the Gaussian distribution property of cipher image. [Rong Huang, Kouichi Sakurai].

3. HASH FUNCTION
Standard secure hash algorithm, many secure algorithm are available depends upon message length SHA are typically used with other cryptographic algorithms for keyed-hash message authentication. one-way hash functions that can process a message to produce a condensed representation called a message digest. 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that gives same message digest. Any change to a message will, with high probability, result in a different message digest.secure hash algorithm can be in two stages: preprocessing and hash computation. Preprocessing is padding a message, parsing the padded message into m-bit blocks, and set initial values to be used in the hash computation. For the secure hash algorithms, the size of the message block - m bits - depends on the algorithm. SHA-256, each message block has 512 bits, which are represented as a sequence of sixteen 32-bit as gensis block.

$$ch(x,y,z) = (x\text{^}y) \oplus (\sim x \wedge z) \quad (1)$$

$$maj(x,y,z) = (x\text{^}y) \oplus (x \wedge z) \oplus (y \wedge z) \quad (2)$$

$$\sum_0^{(256)}(x) = ROTR^2(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x) \quad (3)$$

For SHA-256, the initial hash value, $H(0)$, shall consist of the following eight 32-bit words, $H_0^{(0)}, H_1^{(0)}, H_2^{(0)}, H_3^{(0)}, H_4^{(0)}, H_5^{(0)}, H_6^{(0)}, H_7^{(0)}$. These words were obtained by taking the first thirty-two bits of the fractional parts of the square roots of the first eight prime numbers. The

hash computation generates a message schedule from the padded message and use with functions, constant operations to iteratively generate a series of hash values. The final hash value generated by the hash computation is used to determine the message digest. using SHA will provide high security for proposed algorithm.

4. PROPOSED ALGORITHM:

Color image compression and encryption with secure hash function techniques ,which processing for secure and fast transmission of image.Compression techniques which is storing R,G,B color values only for compressing image and followed by compressed image that leads to encrypt an image using secure transmission function algorithm its is a cryptographic hash function with digest length of 256 bits.

Step 1: Input image as I.

Step2: Convert image to RGB for pre-processing process.

Step3:To compress store RGB values randomly.

Step4: Take a compressed image for encrypt process 512*512 size, convert (m*n) rows and columns for encrypt each pixel with represented bit .create m bit block value..For compute key digest .

Step 5: Then make all zeros m*n for returns an m-by-n matrix of zero and temporary w-bit word for in the hash computation with image size, compare with it.

Step 6:perform ⊕ Bitwise XOR (“exclusive-OR”) operation with 32 bit block for generate digest . **Step 7**: compute hash with bit block amd reverse Bit xor process.

Step 8: Addition modulo 2w.:Z=(X + Y) mod 2w. Right shift operation: SHR n (x)=x >> n,rotate right (circular right shift) operation:ROTR n (x)=(x >> n) Ú (x << w - n). Padded the message,Parising the values into block values 512 blocks i.e,16 times of 32-bit values. The resulting 256-bit message digest of the message.and inverse above steps for decrypt process

Step 8: For decompression process take a each pixel of color as adjacent avearge,the only available color values are taken.

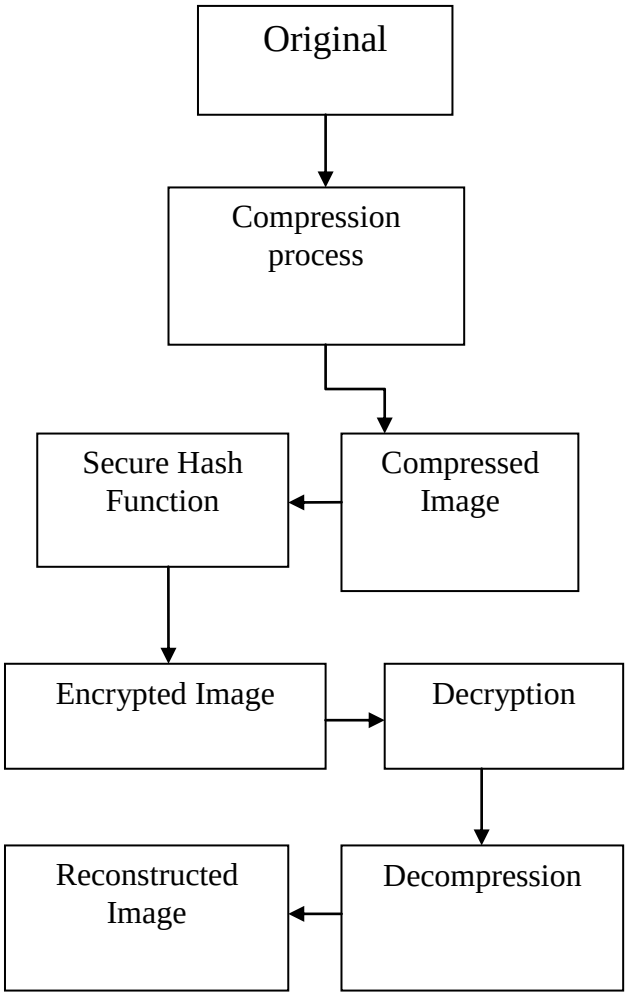
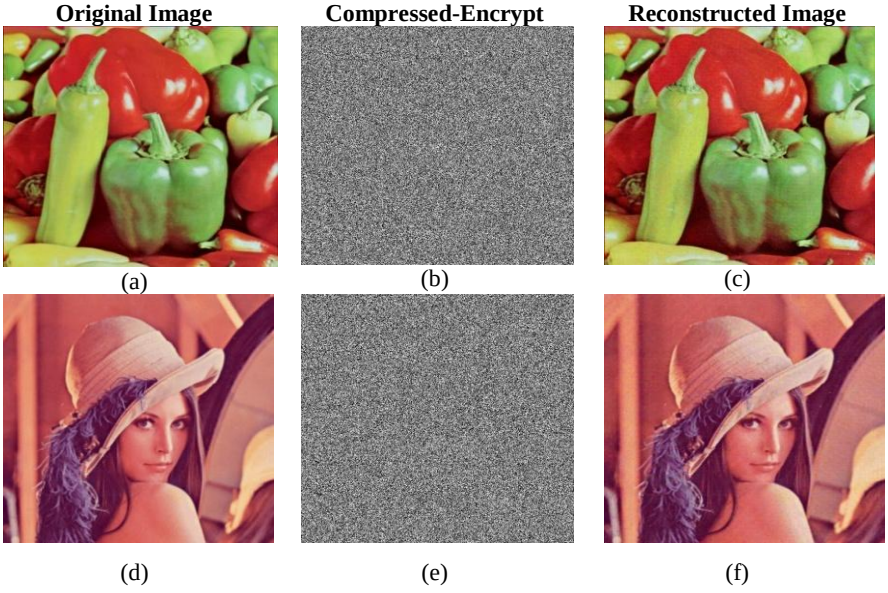
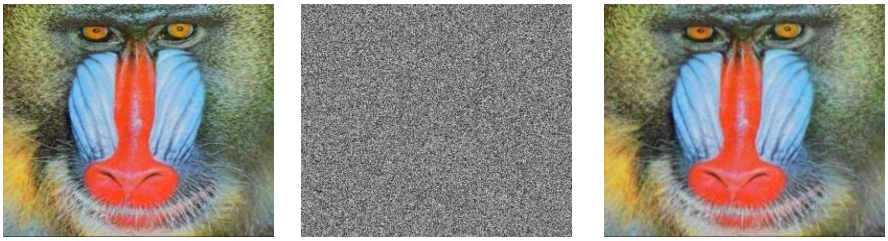


Figure 1: Block Diagram for Proposed work

5. EXPERIMENT AND ANALYSIS





(g) (h) (i)

Figure 2: Original, Compressed-encrypt and Reconstructed Image of Pepper, Lena, Baboon

The various analysis of images have been performed on a Matlab platform. For simplicity, the calculation formula of image correlation coefficient, peak-to-peak signal-to-noise ratio (PSNR) and mean squared error (MSE) . Three plain images ‘‘Lena”, ‘‘Man” and ‘‘Lake” of size 512*512 are designated as test image**.**

5.1 Histogram And Correlation Analysis

Histogram is an important feature of an image, which is used to analysis the performance of image encryption algorithms. Fig. 2(a), (c) and (e) are corresponding histograms of original images, while Fig. (b), (d) and (f) are corresponding histograms of encrypted images and , respectively.The histograms of different encryption images show a Gaussian distribution, though histograms of different original images are apparently different. the statistical analysis attacks by histogram,the proposed image compression-encryption algorithm is secure. In order to verify the security of the proposed algorithm, we test the correlation of adjacent pixels and joint distribution analysis. 10,000 pairs of adjacent pixels in horizontal, vertical, and diagonal directions are randomly selected from the original images and corresponding encrypted images as samples; (2) the correlations between two adjacent pixels are calculated for each direction. Table 1 shows the correlation of adjacent pixels of original images and encrypted images with different methods. The values of the correlation coefficients between two adjacent pixels in the encrypted images are much weaker than those in their corresponding original images. The correlation coefficients between two adjacent pixels in the encrypted images with the proposed algorithm are also smaller than those with the algorithm in [7].

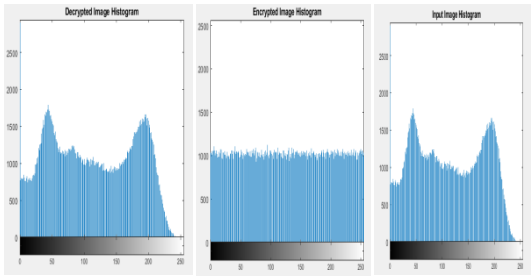


Figure 3. Histrogram for Original lena (a),Encrypt lena(b) , Decrypt lena(c)

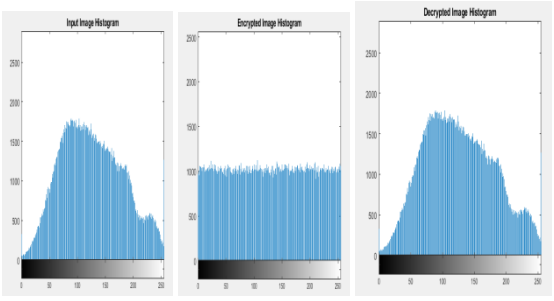


Figure 4. Histogram for Original (a),Encrypt (b),Decrypt for Baboon (c)

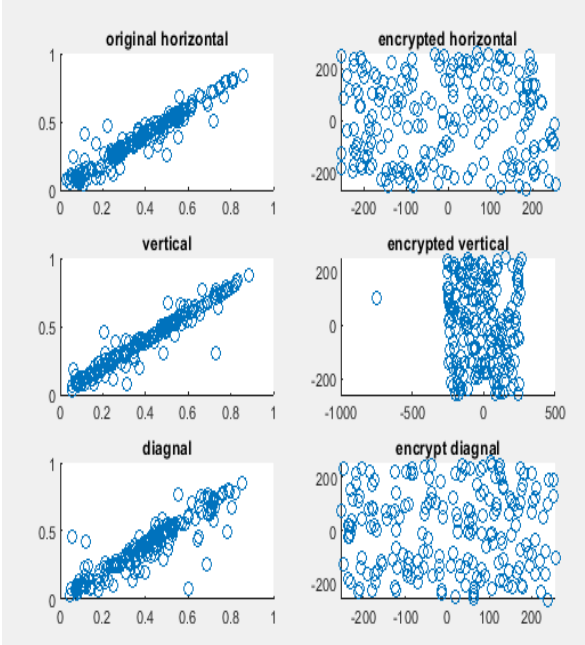


Figure 5.Correlation Co-efficient of plain image and encrypted lena

Table 1 Correlation coefficient of adjacent pixels.

Correlation coefficient	Horizontal direction	Vertical direction	Diagonal direction
‘Lena’	0.9569	0.9236	0.9019
Encrypted lena	0.04005	-0.02158	0.30471
‘Pepper’	0.9647	0.9618	0.9324
Encypted Pepper	0.04401	0.03886	0.00253

5.2 Compression Performance

Compression ration calculated as: Compressio nratio=compressimage/uncompressed image.

Compression ratio of image, the size of the compressed image is 33% as large as plain image ,the quality of the decrypted image is acceptable. Lossy compression ratio is 19:1.In various stage, which means the compression to capable of proposed method is high for transmission.

PSNR Peak to signal noise ratio is calculated as:

PSNR=10log10 $\left(\frac{R^2}{MSE}\right)$

To find better the quality of the compressed, or reconstructed image. The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image compression quality.

MSE is very lower than PSNR in Proposed work. PSNR value as 45.567 for lena reconstructed image fig.1(c) 42.890 for pepper fig.1(f) 47.234 for baboon.fig.1(i)

5.3 Key space

The size of key space shows the difficulty and complexity in attacking a cryptosystem , thus a large enough key space is necessary to against the brute-force attack.

Table 2:Keyspace for different algorithm

Algorithm	Algorithm [4]	Algorithm [7]	Proposed algorithm
Key space	2^{187}	2^{64}	2^{194}

6. CONCLUSION

A image compression and encryption based algorithm for high speed and secure transmission of digital image while passing through web. So the proposed work are highly

achieved as needed speed and security .This proposed work that are to be work with color image for without losing color and detailed information in image ,this work is very useful to modern digital world. Experimental results ,that the proposed scheme is effective, secure and robust to compress encrypt and decompress-decrypt images.

7. REFERENCES

[1] Musheer Ahmad , M.N. Doja , M.M. Sufyan Beg , Security analysis and enhancements of an image cryptosystem based on hyperchaotic system,in press .pp 1-8.

[2] [2] Sattar Mirzakuchaki, Reza Ebrahimi Atani, A Novel Image Encryption Algorithm Based onHash Function. 2010 IEEE. 978-982.

[3] Sergey Krivenko,Nikolay Ponomarenko, : A Comprehensive Study of Lossy Compression of Noisy Images Based on Visual Quality ISSN 1687-6180.

[4] Gong, Lihua; Deng, Chengzhi; Pan, Shumin; Zhou, Nanrun: Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform, Optics and Laser Technology, Volume 103, p. 48-58.

[5] Adem Orsdemir, H. Oktay Altun, Gaurav Sharma, Mark F. Bocko: on the security and robustness of encryption via compressed sensing, IEEE Print ISBN: 978-1-4244-2676-8, Print ISSN: 2155-7578.

[6] Aidi Zhang , Nanrun Zhou: Color Image Encryption Algorithm Combining Compressive Sensing with Arnold Transform, JOURNAL OF COMPUTERS, VOL. 8, NO. 11 PP no-2857-2862.

[7] Rong Huang, Kouichi Sakurai: A Robust and Compression-combined Digital Image Encryption Method Based on Compressive Sensing, 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing pp.no 105-108.

[8] D. Venugopal , M.Gunasekaran , A.Sivanatharaja : Secured Color Image Compression and Efficient Reconstruction Using Arnold Transform with Chaos Encoding Technique, International Journal of Advanced Research in Computer and Communication Engineering Vol. 4 P.169-174.

[9] Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma: Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm, IJCTEE Volume 1, Issue 3 p-no 7-11.

[10] Xiaodong Li , Cailan Zhou , Ning Xu. A Secure and Efficient Image Encryption Algorithm Based on DNA Coding and Spatiotemporal Chaos, International Journal of Network Security, Vol.20, No.1, PP.110-120.

[11] Shubo Liu, Jing Sun , Zhengquan Xu , Jin Liu: Analysis on an Image Encryption Algorithm, International Workshop on Education Technology and Training.

[12] Guodong Ye and Xiaoling Huang: A secure image encryption algorithm based on chaotic maps and SHA-3, Security Comm. Networks 2016; 9:2015–2023 © 2016 John Wiley & Sons, Ltd.

[13] Xingyuan Wanga , Siwei Wanga , Yingqian Zhang ,Chao Luo : A one-time pad color image cryptosystem based on SHA-3 and multiple chaotic systems. Optics and Lasers in Engineering 103 p.no 1–8. R. C. Gonzalea and R. E. Woods, "Digital Image Processing", 2nd Ed., Prentice Hall, 2004.

[14] W.Black ,An introduction to digital image processing ,Strandberg Publishing Company Birkeroed,Denmark,Denmark ,1985.

[15] https://www.mathworks.com/matlabcentral/fileexchange/4718-lossy-image-compression.