Secure Schematic Model for Verifying Encrypted Image using Invariant Hash Function

Smita R. Chunamari
Dept of. Computer Egineering
A. C. Patil College of Egineering Kharghar
Navi Mumbai, India

D. G. Borse
Dept. of Electronic and Telecommunication
A. C. Patil College of Egineering Kharghar
Navi Mumbai, India

ABSTRACT
In post globalization era of computer networks and communication, image and video plays a significance role; rather the fashion of text based systems will be replaced by the image based system. The associated threats and challenges related to image security and its authentication is an active research issues. In order to ensure a full proof security mechanism for image the notion of message authentication code for data authentication and notion of encryption for preserving confidentiality need to be combined. In this paper a complete frame work of crypto-system has been proposed, where the parameterization of hash value of encrypted image is done in such a way that it should be exactly same with zero difference error of hash value that of the parent unencrypted original image. It will have enormous scope into various medical imaging systems where privacy preservation is an important issue. Designing parametric hashing algorithm, which is invariant to encryption only by accepting small part of statistical signature of the original unencrypted image to emerge despite the encryption process is a non trivial task. The proposed work formulates authentication of encrypted data by using notion of authentication code and a novel but yet simple hashing algorithm which are usable with encrypted image s. The implementation results of various images, where the hash value is being computed without the decryption of the original input image, thus validates the authentication without compromising the privacy information. Since the hash value is computed without decrypting the original data, one can prove authenticity without actually revealing the information.

Keyword
Image Encryption, Hash Function, Encryption, Secure Key.

1. INTRODUCTION
The presence of computer networks has prompted new problems with security and privacy. Having a secure and reliable means for communicating with images and video is becoming a necessity and its related issues must be carefully considered. Hence, network security and data encryption have become important. The images can be considered nowadays, one of the most usable forms of information. Image and video encryption have applications in various fields including Internet communication, multimedia systems, medical imaging, telemedicine and military communication [1][2][3]. There are two types of applications for information transmission over the Internet. The first ones are the online applications, which consider the speed as the main issue. The second ones are web pages, which consider the security as the main issue. [4][5]. The security mechanisms which are employed to protect the multimedia data from unauthorized operations are (1) Multimedia encryption to prevent eavesdropping, (2) Watermarking for copyright protection and tracking and (3) Parametric multimedia hashing for content authentication. Recently, with the greater demand for digital world, the security of digital images has become more and more important since the communications of digital products over open network occur more and more frequently [2, 3, 6]. Surveys of the existing work on image encryption were also gave general guideline about cryptography and concluded that all techniques were useful for real-time image encryption. Techniques described in those studies can provide security functions and an overall visual check, which might be suitable in some applications. So no one can access the image which transferring on open network. Multimedia encryption and multimedia authentication schemes serve two different purposes but they can be merged together in one system to protect confidentiality and to check the authenticity of the data. Multimedia hashing is another method employed for authenticating the messages. Hashing is essentially a many-to one mapping which is used to authenticate the message and to ensure that it came from the true source. They are also called as one-way functions because given a message M and a hash function H, it is very easy to compute the hash $h = H(M)$ but given the hash h, it is impossible to compute M such that $h = H(M)$. The robustness requirement of the hash against manipulations is different for content authentication and copyright protection applications as it is for watermarks. The former requires the hash to be fragile against even minute manipulations while the later requires it to be robust even against major manipulations.

The proposed paper discusses about the image authentication and encryption. The section II gives an overview of related work which identifies all the major research work being done in this area. Section III highlights about the image encryption considered in previous research work. Proposed system is discussed in Section IV followed by implementation and results in Section V. Finally section VI gives the conclusion of proposed work and the future extensible work to be done.

2. RELATED WORK
In the digital world nowadays, the security of digital image has become more and more important because of the advances in communication technology and multimedia technology. We can realize that more and more researches have been developed for security issues to protect the data from possible unauthorized instructions [6].The security of digital images involves several different aspects, including copyright protection, authentication, confidentiality, and access control. Generally, the copyright protection is addressed by digital watermarking, which embeds the owner's private information, called the watermark, into the original image and extracts it from a questionable image when the ownership needs to be resolved. On the other hand, content confidentiality and

access control are addressed by encryption, through which only authorized parties holding encryption keys can access content in clear text [7, 8]. In this regard, a direct solution is to use an encryption algorithm to encrypt the data, directly. This solution has led to the number-theory-based encryption algorithms such as the Data Encryption Standard (DES), AES, which is a symmetric encryption algorithms and the RSA algorithm, developed by Rivest, Shamir and Adleman, which is an asymmetric encryption algorithm [9][10][11].

However, these encryption schemes appear not to be ideal for image applications, due to some intrinsic features of images such as the bulk data capacity and high redundancy, which are troublesome for traditional encryption. Moreover, these encryption schemes require extra operations on compressed image data, thereby demanding long computational time and high computing power. In real-time communications, due to their low encryption and decryption speeds, they may introduce significant latency [12].

Innovative encryption techniques need to be developed for effective data encryption for financial institutions, E-commerce, and multimedia applications. For future Internet applications on wireless networks, encryption techniques for multimedia applications need to be studied and developed. In this thesis, we focus on the subject of image encryption. Obviously it can be seen that majority of the work is carried out on image encryption.

3. IMAGE ENCRYPTION

The basic idea of *encryption* is to modify the message in such a way that only a legal recipient can reconstruct its content. A discrete-valued cryptosystem can be characterized by:

- a set of possible plaintexts, P.
- a set of possible cipher texts, C.
- a set of possible cipher keys, K.
- a set of possible encryption and decryption transformations, E and D.

An encryption system is also called ***a cipher***, or a cryptosystem. The message for encryption is called *plaintext*, and the encrypted message is called *ciphertext*. Denote the plaintext and the ciphertext by P and C, respectively. The encryption procedure of a cipher can be described as:

$$C = E_{ke}(P)$$

where E_{ke} is the encryption key and *E* is the encryption function. Similarly, the decryption procedure is defined as:

$$P = D_{kd}(C)$$

where D_{kd} is the decryption key and *D* is the decryption function. The security of a cipher should only rely on the decryption key D_{kd}, since an adversary can recover the plaintext from the observed ciphertext once he/she gets D_{kd}. Figure 1 shows a block diagram for encryption/decryption of a cipher.

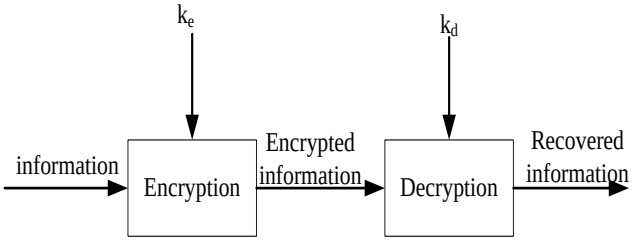

Fig 1 Encryption/Decryption of cipher

Classical encryption algorithms are sensitive to keys, while chaotic maps are sensitive to initial conditions and parameters. Cryptographic algorithms shuffle and diffuse data by rounds of encryption, while chaotic maps spread the initial region over the entire phase space via iterations. Permutations are important mathematical building blocks for symmetric encryption systems in general, and block ciphers in particular. Permutation is a bijective map whose domain and range are the same. Permutation ciphers based on chaos have been proposed [13].

Let $\mathcal{S}$ be a set. A map $f: \mathcal{S} \rightarrow \mathcal{S}$ is a permutation iff is bijective (i.e. injective and subjective). The set of all permutations of $\mathcal{S}$ is denoted by $Perm\mathcal{S} \rightarrow \mathcal{S}$. We employ a permutation cipher based on the Cat map. The Cat map is given by,

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N$$

where, x_n and y_n represent the rows and columns of the data points respectively, N is the number of columns in data block to be permuted. We have taken a block size of 16 × 16 where the data points are actually the DCT coefficients of the image.

The Cat map is employed for a number of iterations for each 16×16 block. The secret key K decides the number of iterations for which Cat map will be employed for each block. The secret key also decides the values of parameters p and q. In our simulations, we have considered 256×256 image. So, in total we are having 256 blocks on which Cat map has to be employed. The inverse Cat map for decryption is given by,

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} pq+1 & -p \\ -q & 1 \end{bmatrix} \begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} \bmod N$$

4. TECHNIQUES OF IMAGE ENCRYPTION

The various techniques of image encryption found in literature till now are classified as following:

- **Modified AES Based Algorithm for Image encryption (2007)**: M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki [14] analyze the Advanced Encryption Standard (AES), and in their image encryption technique they add a key stream generator (A5/1, W7) to AES to ensure improving the encryption performance.
- **Image Encryption Using Block-Based Transformation Algorithm (2008):** Mohammad Ali Bani Younes and Aman [15] introduce a block-based transformation algorithm based on the combination of image transformation and a well known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm, and then the transformed image was encrypted using the Blowfish algorithm. Their results showed that the correlation between image elements was significantly decreased. Their results also show that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy.
- **An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption (2008)**: Mohammad Ali Bani Younes and Aman Jantan [16] introduce a new permutation technique based on the combination of image permutation and a well known encryption algorithm called RijnDael. The original image was divided into 4 pixels × 4 pixels blocks, which were rearranged into a permuted image using a permutation process, and then the generated image was encrypted using the RijnDael algorithm. Their results showed that the correlation between image elements was significantly decreased by using the combination technique and higher entropy was achieved.

- **Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm (2008)**: Saroj Kumar Panigrahy, Bibhudendra Acharya and Debasish Jena [17] present image encryption technique using the Hill cipher. They are generating self-invertible matrix for Hill Cipher algorithm. Using this key matrix they encrypted gray scale as well as colour images. Their algorithm works well for all types of gray scale as well as colour images except for the images with background of same gray level or same color.
- **Image Encryption Using Advanced Hill Cipher Algorithm (2009)**: Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda [18] have proposed an advanced Hill (AdvHill) cipher algorithm which uses an Involutory key matrix for encryption. They have taken different images and encrypted them using original Hill cipher algorithm and their proposed AdvHill cipher algorithm. And it is clearly noticeable that original Hill Cipher can't encrypt the images properly if the image consists of large area covered with same colour or gray level. But their proposed algorithm works for any images with different gray scale as well as color images.
- **Digital image encryption algorithm based on chaos and improved DES (2009):** Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan and Dai Wei-di [19] researches on the chaotic encryption, DES encryption and a combination of image encryption algorithm. In their technique firstly, new encryption scheme uses the logistic chaos sequencer to make the pseudo-random sequence, carries on the RGB with this sequence to the image chaotically, then makes double time encryptions with improvement DES.Their result show high starting value sensitivity, and high security and the encryption speed.
- **New modified version of Advance Encryption Standard based algorithm for image encryption (2010):** Kamali S.H., Shakerian R.,Hedayati M. and Rahmani M.[20] analysis Advance Encryption Standard(AES) algorithm and present a modification to the Advanced Encryption Standard (MAES) to reflect a high level security and better image encryption. Their result so that after modification image security is high. They also compare their algorithm with original AES encryption algorithm.
- **Image Encryption Using Affine Transform and XOR Operation (2011):** Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar and Partha Pratim Sarkar [21] propose a two phase encryption and decryption algorithms that is based on shuffling the image pixels using affine transform and they encrypting the resulting image using XOR operation. They redistribute the pixel values to different location using affine transform technique with four 8-bit keys. The transformed image then divided into 2 pixels x 2 pixels blocks and each block is encrypted using XOR operation by four 8-bit keys. The total key size used in algorithm is 64 bit. Their results proved that after the affine transform the correlation between pixel values was significantly decreased.
- **Permutation based Image Encryption Technique (2011)**: Sesha Pallavi Indrakanti and P.S.Avadhani [22] proposes a new image encryption algorithm based on random pixel permutation with the motivation to maintain the quality of the image. The technique involves three different phases in the encryption process. The first phase is the image encryption. The second phase is the key generation phase. The third phase is the identification process. This provide confidentiality to color image with less computations Permutation process is much quick and effective. The key generation process is unique and is a different process.
- **Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it (2011)**: Kuldeep Singh and Komalpreet Kaur[23] are compared four chaotic maps Cross chaotic, Logistic, Ikeda and Henon map and noise effects are observed on image. Firstly, they use the image encryption algorithm to convert original image to encrypted image. Then they apply noise on the encrypted image and then decrypt cipher image with noise back to original image. They have found out that cross chaotic map showed best results than other three chaotic maps.
- **Image Encryption Based on the General Approach for Multiple Chaotic Systems (2011)**: Qais H. Alsafasfeh and Aouda A. Arfoa[24] proposed new image encryption technique based on new chaotic system by adding two chaotic systems: the Lorenz chaotic system and the Rössler chaotic system. From Experimental analysis they demonstrate that the image encryption algorithm has the advantages of large key space and high-level security, high obscure level and high speed.
- **Image Encryption Using Differential Evolution Approach In Frequency Domain (2011)**: Ibrahim S I Abuhaiba and Maaly A S Hassan[25] present a new effective method for image encryptionwhich employs magnitude and phase manipulation using Differential Evolution (DE) approach. They have carried out key space analysis, statistical analysis, and key sensitivity analysis to demonstrate the security of the new image encryption procedure.
- **Statistical analysis of S-box in image encryption applications based on majority logic criterion (2011)**: Tariq Shah, Iqtadar Hussain, Muhammad Asif Gondal and Hasan Mahmood[26] propose a criterion to analyze the prevailing S-boxes and study their strengths and weaknesses in order to determine their suitability in image encryption applications. The proposed criterion uses the results from correlation analysis, entropy analysis, contrast analysis, homogeneity analysis, energy analysis, and mean of absolute deviation analysis. These analyses are applied to advanced encryption standard (AES), affine-power-affine (APA), gray, Lui J, residue prime, S8 AES, SKIPJACK, and Xyi Sboxes.

5. PROPOSED SYSTEM

In recent the protection of data is required while sending the data in the network. The proposed system highlights a secure image encryption and authenticating the encrypted data. The proposed algorithm calculates hash value of data (image) so that the encryption process remains transparent to the Hash function. The Model of navigation, in order to showcase the complete framework of encryption-description of an image is as below shown in figure number. A hash function h(m) is a message digest; in some sense, the message is condensed. Hash functions are routinely used to check integrity or for error detection of transmitted messages. Hash functions should accept messages of any length as input, produce a fixed-length output, and be fast. Message authentication codes (MAC) check both integrity and authenticity. MACs require the parties in the communication to agree on an algorithm and possess a secret key. The MAC algorithm uses the secret key and the message as input, and it outputs a message authentication code.

The mathematical representation of the hash calculated using the plaintext data and the encrypted data will remain the same and can be represented as given below in the equation

$$H_{ash}\,(E_{nc}\,(msg, E_k), K_h) = H_a(msg, K_h)$$

Where, *msg* the message to be transmitted, E_{nc} is the encryption function, E_k the encryption key, K_h the hashing key and H_a the hashing algorithm. It also to be ensure that

$$H_{ash}\,(E_{nc}\,(msg, E_{k1}), K_h) = H_{ash}\,(E_{nc}\,(msg, E_{k2}), K_h)$$

Where, E_{k1} and E_{k2} are two encryption keys. To start with, first to compute the 16x16 block Discrete Cosine Transform (DCT) of the image. In order to do that, first divide the image into blocks each of dimension of order 16x16 and after dividing there will be total 256 such blocks. For the N^{th} block I_N the 2-dimensional DCT D_N is given as,

$$D_N = a_i a_j \sum_{m=0}^{15}\sum_{n=0}^{15} I_{Nij} \cos\frac{\pi(2mH)i}{2M} \cos\frac{\pi(2nH)j}{2N}$$

Where $0 \le i \le 15, 0 \le j \le 15$ and

$$a_i = \begin{cases} \frac{1}{4} & i = 0 \\ \frac{1}{\sqrt{8}} & 1 \le i \le 15 \end{cases} \text{ and } a_i = \begin{cases} \frac{1}{4} & j = 0 \\ \frac{1}{\sqrt{8}} & 1 \le j \le 15 \end{cases}$$

After calculating the DCT coefficients for each block and then apply the Cat map individually to each of the block. The secret key decides the values of the parameters p and q and the number of iterations for which Cat map will be employed for each of the block. Applying a permutation cipher which scrambles only the positions of the DCT coefficients within the block, the statistics of the block like its mean and variance remain the same. So, in order to generate the hash, select the means and variances of the blocks as proposed feature space. This feature space remains invariant to the encryption process. Hence, the hash of the original image and the scrambled image remain the same. The mean of the N^{th} block D_N is given by,

$$mean_{D_N} = \frac{1}{256}\sum_{i=0}^{15}\sum_{j=0}^{15} D_N(i,j)$$

The means and the variances are normalized using the following equations,

$$\text{var}_{D_N} = \sum_{i=0}^{15}\sum_{j=0}^{15} \{D_N(i,j) - mean_{D_N}\}^2$$

$$norm\_mean_{DK} = \frac{mean_{D_K}}{\max\limits_{k \in \{1,2,..256\}} \{mean_{D_K}\}}$$

$$norm\_\text{var}_{DK} = \frac{\text{var}_{D_K}}{\max\limits_{k \in \{1,2,..256\}} \{\text{var}_{D_K}\}}$$

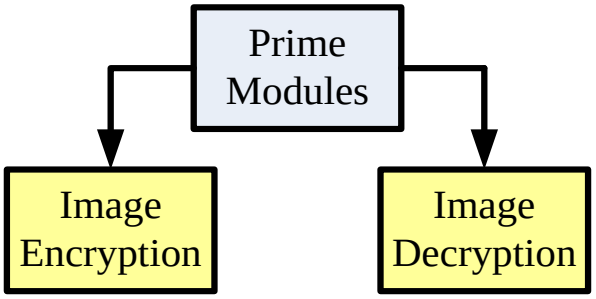

Fig 2 Modules of the proposed system.

Cryptographic hash functions and block ciphers are often used to construct MAC algorithms. The modules of the proposed system is as shown in Figure 2:

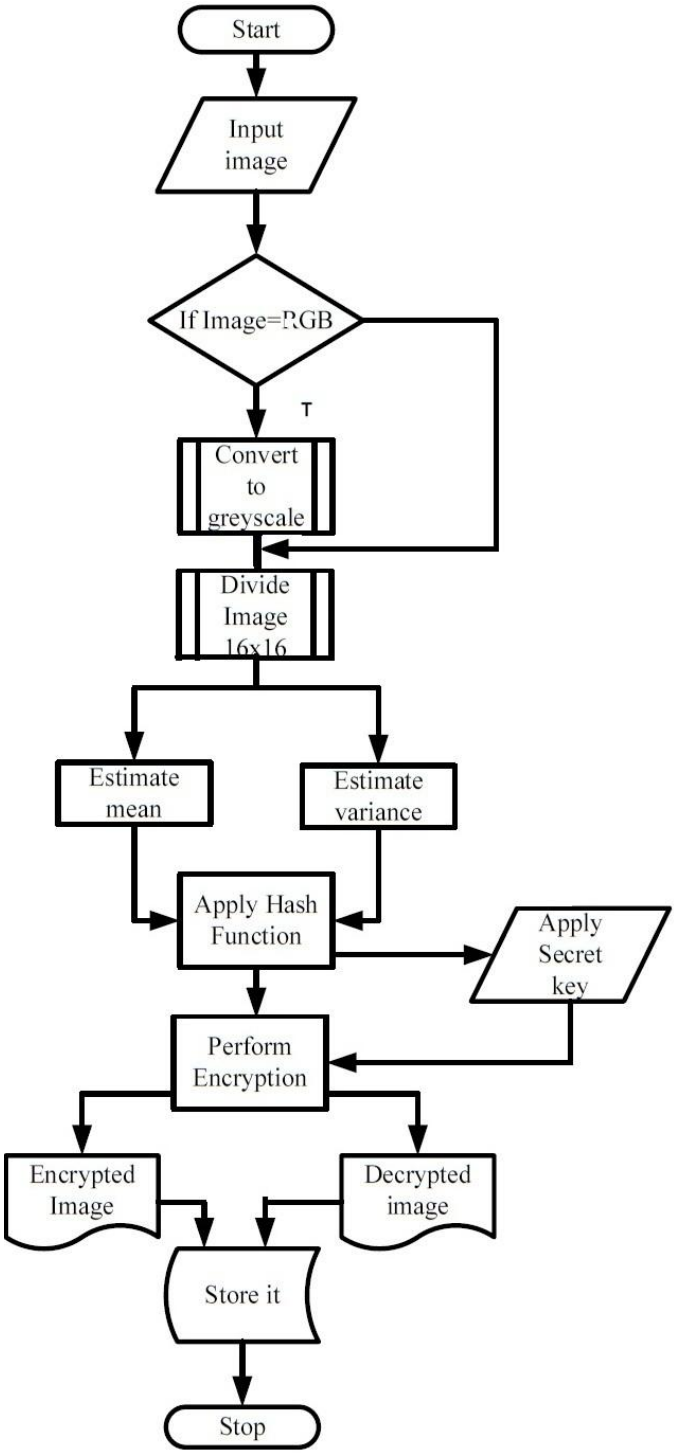

Fig 3 Process Flow Diagram of Proposed System

The complete process flow (Figure 2) of encryption and generation of hash is as shown in figure 3:

So, by using above equations the feature space the normalized means and variances of 256 blocks where, norm_mean_{DK} and mean_var_{DK} $\epsilon(0, 1)$. Next to sort out the blocks based upon the increasing values of the normalized variances. K_h has two components- K_{h1} and K_{h2}.The top n blocks are selected based upon the secret key K_{h1}. The means and variances of the selected blocks are then quantized.

Suppose one of the normalized mean values is 0.7924. The binary equivalent of 0.7924 is 0.11001010110110101. The bit patterns that obtain after quantizing the variance and mean are concatenated together. The concatenated bit patterns obtained for each block are stacked together in a vector P then, using the key K_{h2}, can generate the random sequence between 0 and 1 of length 100. Then, multiply each of the random number with the size of vector P and round off the products. The bits corresponding to the indices indicated by the rounded-off products are selected from the vector P. This is the required hash.

The above calculations are done for the images and the encrypted data and the resultant hashes are found to be the same as shown in Figure 4.

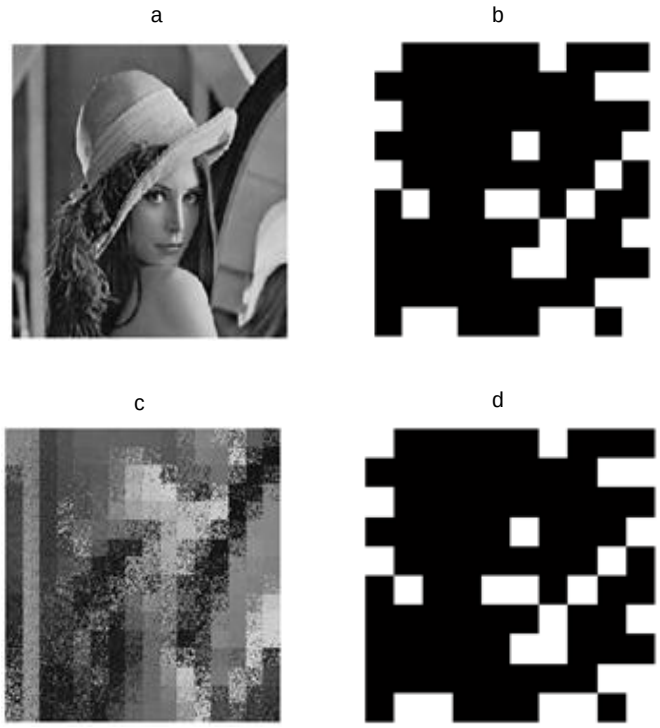

Fig 4. Results showing the validity of the proposed algorithm.

Figure 4 shows the hash of the original image and the encrypted image are same. (a) is the Original Lena image, (b) is the Hash derived from Original Lena image, (c) is the Encrypted Lena image, (d)shows the Hash derived from Encrypted Lena image.

The complete architecture is shown in Figure 5 and the complete process flow of decryption with hash function framework is as shown in Figure 6:

The entire process of decryption is just a reversible process of encryption being performed. The user will require encrypted image, encrypted hash image and secret key to perform decryption. The architectural diagram of decryption process is as shown into the Figure 6

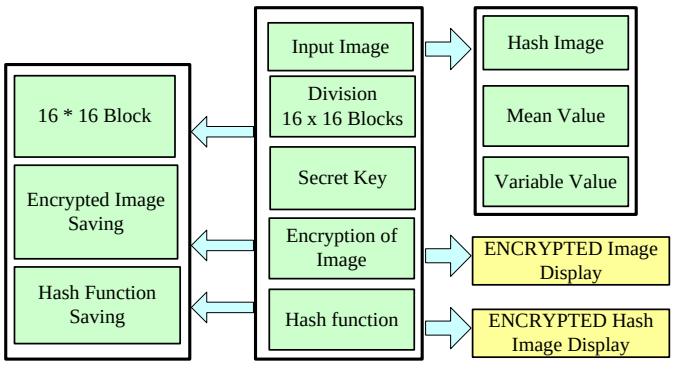

Fig 5 Architectural Schema of Encryption Process.

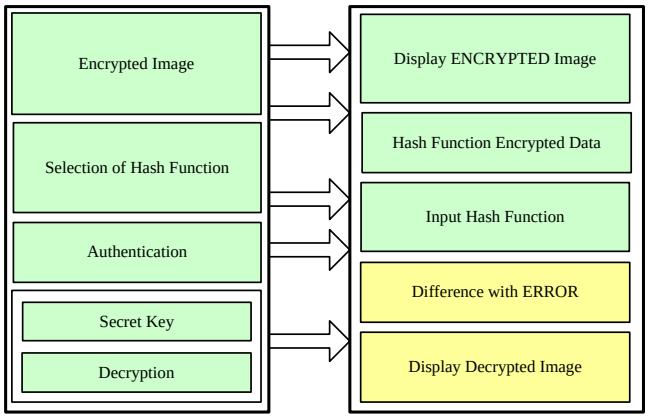

Fig 6 Architectural Schema of Decryption

6. IMPLEMENTATION & RESULTS

In order to show the credibility of the proposed algorithm, it can be tested across a variety of images such that:

- The hash value is unique to a given image. Different images should yield significantly different hash values. If the distance between hash values from two different images are significantly different, this can be used as a means of indexing the respective images.
- The hash invariance to encryption must be verified for different images in order to justify this generalization.

The implementation of the proposed work is shown in Figure 8 and Figure 9. For each image, first compute the 16 × 16 block DCT. Then, each block is encrypted. Chaos encryption based on Cat map has been employed. The key E_k decides the values of p, q and the number of times the Cat map will be iterated for each of the blocks. The security is strong because not only the parameters p, q are decided by the key but proposed work also have randomized the number of iterations for the Cat map.

The next step is to calculate the hash value of the original image and its corresponding encrypted version. As expected, they are found to be the same. The hashes obtained for each of the images are of 100 bits length. It can also be verified that the Hash for any image obtained from the proposed algorithm is unique. It can be ensured by finding the hamming distance between the hashes of different images and then XOR the two hashes.

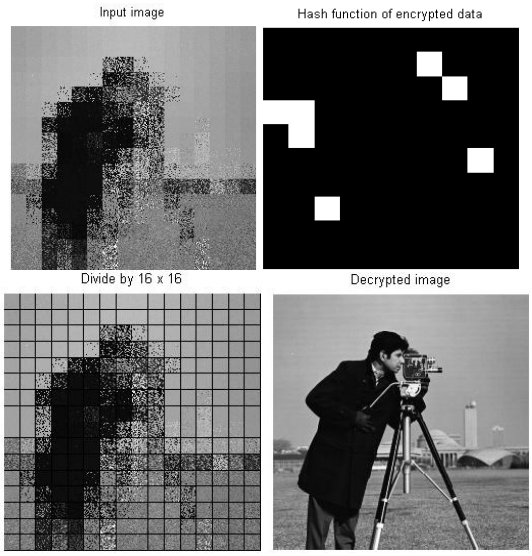

Fig 7 Results of Decryption

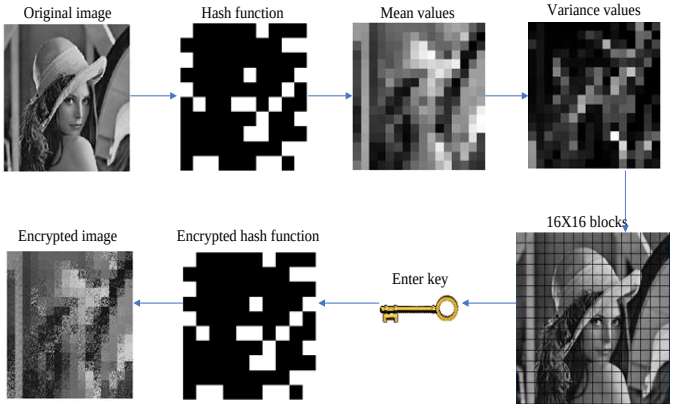

Fig 8 Encryption of original image and the hash functions.

The Figure 8 explains about the original image and its hash function, mean values, variance values and next it converted to a 16x16 block and enter the secret key. After entering the secret key the encrypted hash function and the encrypted original image are shown.

The Figure 7 and Figure 9 explains about the decryption of the image, while in decryption first step is to enter the secret key and then the decrypted hash function and the encrypted image is generated and in next again converted to 16x16 block to retrieve the original image.

7. CONCLUSION

This paper discusses about a new framework for authenticating encrypted images. By allowing a portion of the statistical signature in the original image to surface despite the encryption operation, it becomes possible to validate the authenticity of the encrypted image without tapping into its contents. By constraining the encryption process to be a block DCT permutation cipher, it has been observed that the mean and variances of the blocks remain the same even after encryption. The proposed work has used these two features to construct the hash value. This simple choice of features also depicts a significant variability across a variety of images. Future work entails developing hashes for much stronger ciphers.

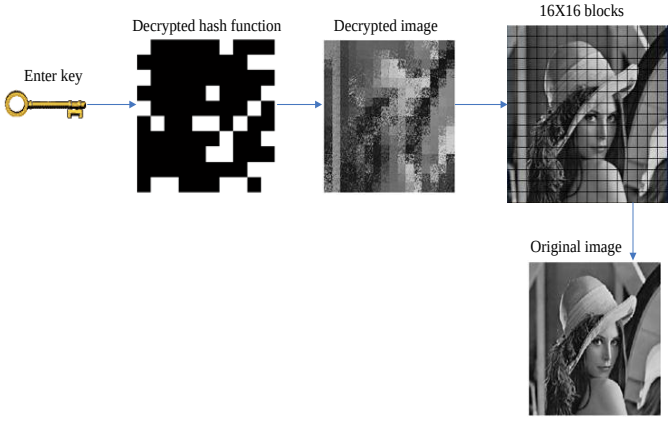

Fig 9 Decryption of the image

8. REFERENCES

[1] O. S. Faragallah, Utilization of Security Techniques for Multimedia Applications , Ph. D. Thesis, Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menofia University, 2007.

[2] A. J. Menezes, P. C. V. Oorschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press Boca Raton,USA, 1996.

[3] L. Qiao, Multimedia Security and Copyright Protection , Ph. D. Thesis, Department of Computer Science, University of Illinois at Urbana-Champaign, Urbana, Illinois, USA, 1998.

[4] W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice- Hall Upper Saddle River, USA, 1999.

[5] C. E. Shannon, Communication Theory of Secrecy Systems, Bell System Technical Journal, Vol. 28, No. 4, pp. 656-715, October 1949.

[6] S. Li, G. Chen and X. Zheng, Chaos-Based Encryption for Digital Images and Videos, Chapter 4 in Multimedia Security Handbook, CRC Press LLC, February 2004.

[7] Y. Mao and M. Wu, A Joint Signal Processing and Cryptographic Approach to Multimedia Encryption, IEEE Transactions on Image Processing, Vol. 15, No. 7, pp. 2061-2075, July 2006.

[8] Y. Mao, Research on Chaos-Based Image Encryption and Watermarking Technology, Ph. D. Thesis, Department of Automatation, Nanjing University of Science & Technology, Nanjing, China, August 2003.

[9] J. Daemen and V. Rijmen, AES Proposal: Rijndael, AES Algorithm Submission, 1999.

[10] R. L. Rivest, M. J. B. Robshaw, R. Sidney, and Y. L. Yin, The RC6TM Block Cipher , M. I. T laboratory for Computer Science, 545 Technology Square, Cambridge, MA 02139, USA, 1998.

[11] R. F. Sewell, Bulk Encryption Algorithm for Use with RSA , Electronics Letters , Vol. 29, No. 25, pp. 2183-2185, 9 Dec. 1993.

[12] H. E. H. Ahmed, H. M. Kalash, and O. S. Faragallah, Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images , International

Conference on Electrical Engineering (ICEE '07), pp. 1-7, 11-12 April 2007.

[13] Z. Lv, L. Zhang, and J. Guo, "A Symmetric Image Encryption Scheme Based on Composite Chaotic Dispersed Dynamics System," *Proc. Of Second Symposium on Computer Science and Computational Technology*, pp. 191–194, 2009.

[14] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, R. Tourki, ―A Modified AES Based Algorithm for Image Encryption‖, World Academy of Science, Engineering and Technology 27 2007.

[15] Mohammad Ali Bani Younes and Aman Jantan ―Image Encryption Using Block-Based Transformation Algorithm‖ IAENG International Journal of Computer Science, 35,2008.

[16] Mohammad Ali Bani Younes and Aman Jantan, ―An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption‖, IJCSNS International Journal of Computer Science and Network Security, VOL.8 , April 2008.

[17] Saroj Kumar Panigrahy, Bibhudendra Acharya and Debasish Jen‖, Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm 1st t International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008.

[18] Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda, Image Encryption Using Advanced Hill Cipher Algorithm, International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.

[19] Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan , Dai Wei-di, Digital image encryption algorithm based on chaos and improved DES‖, IEEE International Conference on Systems, Man and Cybernetics, 2009.

[20] Kamali, S.H., Shakerian, R., Hedayati, M.,Rahmani, M., A new modified version of Advance Encryption Standard based algorithm for image encryption, Electronics and Information Engineering (ICEIE), 2010 International Conference.

[21] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar Partha Pratim Sarkar, ―Image Encryption Using Affine Transform and XOR Operation‖, International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011).

[22] Sesha Pallavi Indrakanti, P.S.Avadhani, Permutation based Image Encryption Technique, International Journal of Computer Applications (0975 – 8887) Volume 28– No.8, 2011.

[23] Kuldeep Singh, Komalpreet Kaur, Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it‖, International Journal of Computer Applications (0975 – 8887) Volume 23– No.6, June 2011.

[24] Qais H. Alsafasfeh , Aouda A. Arfoa, Image Encryption Based on the General Approach for Multiple Chaotic Systems, Journal of Signal and Information Processing, 2011.

[25] Ibrahim S I Abuhaiba, Maaly A S Hassan, ―Image Encryption Using Differential Evolution Approach In Frequency Domain‖ Signal & Image Processing: An International Journal (SIPIJ) Vol.2, No.1, March 2011.

[26] Tariq Shah, Iqtadar Hussain, Muhammad Asif Gondal , Hasan Mahmood, Statistical analysis of S-box in image encryption applications based on majority logic criterion, International Journal of the Physical Sciences Vol. 6(16), pp. 4110-4127, 18 August, 2011