IMPLEMENTATION OF ROBUST SYSTEM TO GENERATE AUTHENTICATED ENCRYPTION FOR SECURE MESSAGE

Mr. Shaikh S.I.[1], Mr. Bhillare P.B.[2], Mr.Kulkarni P.R.[3]

[1]*H.O.D., Information Technology, M.S.Polyechnic Beed, Maharashtra, India*
[2]*H.O.D., Computer Engineering, Aditya Polytechnic Beed, Maharashtra, India*
[3]*H.O.D., Computer Engineering, M.S.Polytechnic Beed, Maharashtra, India*

ABSTRACT

The purpose of this project was to boost the data security focusing on the tow levels of security, namely multimedia encryption and multimedia authentication. The aim is to propose a key-dependent function that returns the same numbers or bits from images and their encrypted versions. By incorporating encryption and hashing in one system, we can have two levels of security and we can prove the authenticity of the data without actually revealing the information. A discrete cosine transform (DCT) expresses a sequence of finitely many data points in terms of a sum of cosine functions oscillating at different frequencies. Watermark is a recognizable image or pattern that appears as various shades of lightness/darkness when viewed by transmitted light, caused by thickness or density variations. A hash function is any algorithm or subroutine that maps large data sets of variable length, called keys, to smaller data sets of a fixed length. Firstly, image is encrypted. For each image, first we compute the 16 × 16 block DCT. Then, each block is encrypted. Decryption is done on encrypted image. Finally, done the image comparison for an input image and an output image with the help of histogram. And the result obtained as expected.

Keyword : *DCT,IDCT,DFT,MAC,AES,DES,PSNR,MSE.*

1. INTRODUCTION

With the growth of the internet and the multimedia technology becoming ubiquitous more than ever, the security of digital images and videos have become more and more important. Multimedia data such as images, videos or audios can be easily copied or accessed by unauthorized users. They have become vulnerable to illicit signal processing operations. The security mechanisms which are employed to protect the multimedia data from unauthorized operations are Multimedia encryption to prevent eavesdropping, watermarking for copyright protection and tracking and parametric multimedia hashing for content authentication. In information technology era, images play important role in representing information. Images can be transmitted through public channel such as internet and also stored in the storage devices. Storage or transmission of images through transmission channels in the form of plain-images have has risks.

1.1 EXISTING SYSTEM

Our existing system described in order to improve the data security, we focuses on the two levels of security. Multimedia encryption and multimedia authentication schemes related to two different purposes but here we merged hem together in one system to protect confidentiality and to check the authenticity of the data. It is indeed a very challenging problem but if we can integrate the two functionalities at a time, it will revolutionize the area of multimedia distribution. The encryption and watermarking operations are done on the same data part. Commutative watermarking and encryption scheme is proposed for providing the media data protection. In this scheme, the partial encryption algorithm is adopted to encrypt the significant part of media data, while some other part is watermarked. It has been observed that commutative schemes based on partitioning the data are vulnerable to replacement attacks. Since one data part is not encrypted, it leads to leakage of information and it is vulnerable to watermark attacks.

1.2 PROPOSED SYSTEM

We propose to integrate the two in a framework where the parameterized hash value of an encrypted image is same as the hash value of the parent unencrypted original image. In watermarking, detection algorithm has been proposed which is able to detect the watermark separately whether it is embedded in the plaintext and after that the watermarked data is encrypted or first the plaintext is encrypted and then the encrypted data is watermarked. Watermark is detected without the decrypting key. But, the encryption permutes only the first 25 DCT coefficients. This is a weak encryption and the encrypted image leaks some information about the original image.

2. LITERATURE REVIEW

Broadband communication networks and multimedia data available in a digital format created many challenges and opportunities for innovation. It makes possible for consumers from all around the world to create and exchange multimedia data due to Versatile and simple-to-use software and decreasing prices of digital devices. Broadband Internet connections and error-free transmission of data gives facility to people to distribute large multimedia files and make identical digital copies of them. Digital watermarking is alternative method to enforce intellectual property rights and protect digital media from tampering. Digital watermarking is defined as robust and secure communication of data. Recently it has been proposed for authentication of both video data and images and for integrity verification of visual multimedia. In such applications, the watermark has to depend on the original image and the secret key. It is important that the dependence on the key be sensitive, while the dependence on the image be continuous that is robust.

2.1 SYSTEM ANALYSIS

Requirement gathering in this stage, all the important issues of usage of encryption, hash function, DCT usage, performing image blocking will be gathered. All the previous techniques will be evaluated before starting coding process. The analysis phase involves gathering requirements for the system. There are several activities that must occur within the analysis phase.

2.1.1A Discrete Cosine Transforms (DCT)

A discrete cosine transform (DCT) expresses a sequence of finitely many data points which is sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression of audio (e.g. MP3) and images (e.g. JPEG), to spectral methods for the numerical solution of partial differential equations. The use of cosine rather than sine functions is critical in these applications: for compression, it turns out that cosine functions are much more efficient. Whereas for differential equations the cosines express a particular choice of boundary conditions.

2.1.2 Watermark

Watermark is a recognizable image or pattern in paper that appears as various shades of lightness/darkness when viewed by transmitted light, caused by thickness or density variations . There are two main ways of producing watermarks; the dandy roll process, and the more complex cylinder mould process. A watermark is very useful because it can be used for dating, identifying sizes, mill trademarks and locations, and the quality of a paper. Encoding an identifying code into digitized music, video, picture or other file is known as a digital watermark. Due to the nature of multimedia objects, security issues are often interleaved with signal processing issues. In particular, security requirements are often stated in an imprecise way using natural language, and attacker models are often too simplistic. This makes it very difficult to assess the security of the schemes when, in real life, the attackers are very creative intelligent [7][12][20]. A quick scan of the available literature shows that the majority of papers have images as their target i.e. audio-visual object [12][22][23]. This silent assumption between security and watermarking is also reflected by the effort put into designing attack tools and the title of a number of conferences e.g. “Security and Watermarking of Multimedia Content”, San Jose. Also the two main industrial applications of watermarking have a focus on security. Whether or not this strong perceived relationship between security and watermarking is beneficial to the deployment of watermarking remains to be seen [5][19][18].

2.1.3 Hash Function

A hash function is defined as any algorithm/subroutine that maps large data sets of variable length, called keys, to smaller data sets of a fixed length. Hash functions are used to accelerate table lookup or data comparison tasks such as detecting duplicated or similar records in a large file, finding items in a database, finding similar stretches in DNA sequences, and so on. In many programming languages this is a contract that allow the user to override equality and hash functions for an object i.e. if two objects are equal, their hash codes must be the same. Hash functions are related to checksums, error correcting codes, check digits, fingerprints, randomization functions, and cryptographic has functions. The Hash Keeper database maintained by the American National Drug Intelligence Center, for instance, is more aptly described as a catalog of file fingerprints than of hash values.

2.1.4 Encryption

In cryptography, encryption is the process of transforming information using an algorithm to make it unreadable to anyone except those who has special knowledge, usually referred to as a key. The result of the process is encrypted information. The reverse process, i.e., to make the encrypted information readable again, is referred to as decryption. Cryptographic algorithms shuffle and diffuse data by rounds of encryption, while chaotic maps spread the initial region over the entire phase space via iterations [22]. Permutations are important mathematical building blocks for symmetric encryption systems in general, and block ciphers in particular. A new and efficient way to deal with the intractable problem of fast and highly secure image encryption is the chaos-based encryption. Therefore, chaotic dynamics are expected to provide a fast and easy way to build cryptosystems. The general Cat map is a two-dimensional invertible chaotic map. N is the width or height of the image. One obtains a two-dimensional Cat map as follows: The Cat map is a bijection set. The chaotic map finally described as follows:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \bmod N \qquad (1)$$

2.1.5 Authenticated Encryption

An authenticated encryption scheme is a symmetric encryption scheme that provide both privacy and integrity. We consider two possible notions of authenticity for such schemes, namely integrity of plaintexts and integrity of ciphertexts, and relate them to the standard notions of privacy by presenting implications and separations between all notions considered. We then analyze the security of authenticated encryption schemes designed by generic composition," meaning making blackbox use of a given symmetric encryption scheme and a given MAC. Three composition methods are considered, i.e. Encrypt-and-MAC, MAC-then-encrypt, and Encrypt-then-MAC.

3. SYSTEM DEVELOPMENT

3.1 SYSTEM DESIGN

An explicit system analysis as well as system design will be prepared for understanding the feasibility of the project planning stages. Design a function for performing hash operation using 16x16 blocks and DCT. Normalized values should then be sorted and quantized. Create a function for encryption using the designed hash function. Perform encryption on data and get random permutation indexes based on secret Key. Design a module that can store the encrypted image as well as hash value in image format. The designed symmetric image encryption scheme employs the chaotic map and general Cat map to process the original image independently. By confusing and diffusing transform, the positions and grey values of image pixels have been shuffled and increase its resistance to various attacks such as the statistical and differential attacks. The test and security analysis demonstrate the high security and fast speed of the new image encryption scheme. which is satisfied both high security and effectively needs is a difficult work.

3.1.1 Activity Diagram for Encryption

The dynamic modeling language, activity diagram shows the encryption technique.

- Input image represents we can input original image.
- The hash value should be unique to a given image because different images should yield significantly different hash values. It creates the mean and variance along with hash image.
- First we compute the 16 × 16 block DCT. Then, each block is encrypted.

- The key K decides the values of p, q and the number of times. The security is strong because not only the parameters p and q are decided by the key but we also have randomized the number of iterations for the picture..
- The hashes obtained for each of the images is of 100 bits length. They are shown in the form of images of dimension 10×10.
- We save the original image's hash image and the encrypted image later need for authentication.

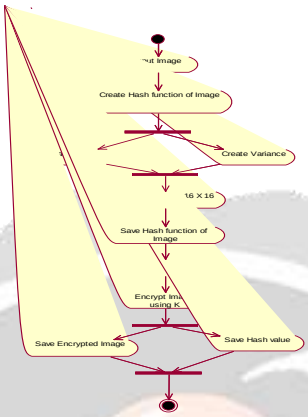

Fig 3.1: Activity diagram for Encryption

3.1.2 Activity Diagram for Decryption

The dynamic modeling language, activity diagram shows the decryption technique.

- Input encrypted image represents that we want to verify.
- Browse the original image's hash function so that invariance to encryption must be verified for different images in order to justify this generalization.
- Authentication of two hash images.
- Before decryption, first once again we have to compute the 16 × 16 block DCT. Then, each block is decrypted.
- The key K decides the values of p, q and the number of times. The security is strong because not only the parameters p and q are decided by the key but we also have randomized the number of iterations for the picture.
- If the key matches the image is decrypted.

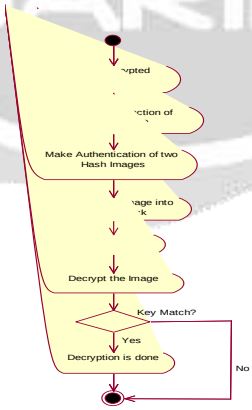

Fig 3.2: Activity diagram for Decryption of image

3.2 SYSTEM IMPLEMENTATION

The implementation phase of any project development is the most important phase as it yields the final solution, which solves the problem at hand. The implementation phase involves the actual execution of the ideas, which are expressed in the analysis document and developed in the design phase.

3.2.1 Problem Formulation

Let the original media be P, the encryption process be represented as E, the watermark embedding algorithm be represented as Wembed , watermark extraction algorithm be represented as Wextract, the watermark be W, the watermark key be Kw, , the encryption key be K, watermarked media be Pw then mathematically,

$$E(W_{embed}(P,W, K_w), K)= E(P_w, K)=P_{w,encrypt} \quad (2)$$

We see that the watermark to remain invariant to the encryption process. That is to say, we want a scheme where in we can extract the watermark without decrypting the received data mathematically,

$$W_{extract}(P_{w,encrypt}, K_w) = W \quad (3)$$

Drawback in Watermarking that watermarks can operate in a stand-alone environment and watermarking for content recognition actually amounts to adding redundancy. Hash functions are one way functions which accepts a variable length message M as input and produces a fixed size output called the hash code H (M). This hash value is appended to the message at the source. The receiver authenticates then this value. When we are concerned with the confidentiality the message by recalculating the hash of communication, w e need to scramble the information using an encryption algorithm and a secret key K. We can preserve some of its attributes while scrambling the data, then these attributes can be used to generate the hash. So, the hash calculated using the plaintext data and the encrypted data will remain the same. Mathematically, it can be stated as,

$$H (E(M , K), K_{hash})= H(M ,K_{hash}) \quad (4)$$

Where, M the message to be transmitted, E is the encryption function, K the encryption key, K_{hash} the hashing key and H the hashing algorithm. Note here by introducing a hashing key K_{hash} we have parameterized the hash value. Thus the hash digest which is obtained becomes equivalent to a message authentication code (MAC). Only the users who share the key K with the source and also possess either the encrypted or original image will be able to verify the hash value. We also have to ensure that

$$H(E(M ,K_1), K_{hash})= H(E(M,K_2),K_{hash}) \quad (5)$$

Where, K_1 and K_2 are two encryption keys. Once we ensure that, we have a scheme wherein zero knowledge proof of data being authentic or not can be given. Such a hash remains invariant to encryption.

3.2.2 Encryption

Encryption enables the scrambling of the data in such a way that it conceals the statistical information and the dependencies in the original plaintext. Traditional encryption algorithms like AES, DES have been employed for multimedia signals but have been found to be computationally intensive particularly when applied to large streams of data such as videos and audio clips. Chaos based encryption algorithms which are much simpler than the traditional encryption algorithms have been used. It excites the scientific community because of the various similarities between chaos based systems and encryption. Cryptographic algorithms shuffle and diffuse data by rounds of encryption, instead chaotic maps spread the initial region over the entire phase space with iterations. In general permutations are important mathematical building blocks for symmetric encryption systems 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 [24].

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

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \quad (6)$$

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 . The data points are 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 and also decides the values of parameters $p$and q.In our simulations, we have considered 256×256 image. So, totally we are having 256 blocks on which Cat map has to be employed. The inverse Cat map for decryption is given by,

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & -p \\ -q & pq+1 \end{bmatrix} \begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} \bmod N \qquad (7)$$

3.2.3 Algorithm for calculating invariant Hash

We propose a novel algorithm to calculate the hash value of the data so that the encryption process remains transparent to the Hash function. Mathematically,

$$H(E(M, K), K_{hash}) = H(M, K_{hash}) \qquad (10)$$

where, M the message to be transmitted, E is the encryption function, K the encryption key, $Khash$ the hashing key and H the hashing algorithm. We also have to ensure that

$$H(E(M,K_1), K_{hash}) = H(E(M,K_2), K_{hash}) \qquad (11)$$

where, $K_1$and $K_2$are two encryption keys. To start with, first we compute the 16x16 block DCT of the image. In order to do that, first we divide the image into blocks each of dimension16x16.In total, we have 256 such blocks. For the k^{th} block, the 2-dimensional DCT $B_k$is given as,

$$B_{k_{ij}} = a_i a_j \sum_{m=0}^{15} \sum_{n=0}^{15} A_{k_{ij}} \cos\frac{\pi(2m+1)i}{2M} \cos\frac{\pi(2n+1)j}{2N} \qquad (12)$$

where, 0 <= i< = 15, 0< = j<= 15 and

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

After calculating the DCT coefficients for each block, we 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. Since, we are 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, we select the means and variances of the blocks as our 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 k^{th} block Bk is given by,

$$mean_{B_k} = \frac{1}{256} \sum_{i=0}^{15} \sum_{j=0}^{15} B_k(i,j) \qquad (13)$$

The variance of the k^{th} block $B_k$is given as,

$$Var_{B_k} = \sum_{i=0}^{15} \sum_{j=0}^{15} \{B_K(i,j) - mean\ B_k\}^2 \qquad (14)$$

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

$$norm_{mean} B_k = \frac{mean B_k}{\max_{k\in\{1,2....256\}}\{mean\ B_k\}} \qquad (15)$$

$$norm\_Var_{B_k} = \frac{Var B_k}{\max_{k\in\{1,2....256\}}\{Var B_k\}} \qquad (16)$$

Key sensitivity test :

Assume that a 16-character ciphering key is used. That is the key consists of 128 bits. A typical key sensitivity test has been performed, accordingly

1. Firstly, a 3000 - 4000 image is encrypted by using the test key ‘‘1234567890123456’’.
2. Then, the least significant bit of the key is changed, so that the original key becomes, say ‘‘1234567890123457’’ in this example, which is used to encrypt the same image.
3. Finally, the above two ciphered images are compared which are encrypted by the two slightly different keys.

The result is the image encrypted by the key ‘‘1234567890123456’’ has 99.61% of difference from the image encrypted by the key ‘‘1234567890123457’’ in pixel grey-scale values, although there is only one bit difference in the two keys. Moreover, when a 16-character key is used to encrypt an image while another modified key is used to decrypt the ciphered image, the decryption also completely fails. Which clearly shows that the image encrypted by the key ‘‘1234567890123456’’ is not correctly decrypted by using the key‘‘1234567890123457’’ there, which has also only one bit difference between the two keys[17].

4. PERFORMANCE ANALYSIS

4.1 SIMULATION RESULT

As the hash value should be unique to a given image. Different images should yield significantly different hash values. If the distance between 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 results explore a new framework for authenticating encrypted images. 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. . In [21], watermarking detection algorithm has been proposed which is able to detect the watermark. Watermark is detected without the decrypting key. But, the encryption permutes only the first 25 DCT coefficients. This is a weak encryption and hence some information can be leaked by the encrypted image about the original image. Where as by using Hash functions, it is the one way functions which accepts a variable length message M as input and produces a fixed size output called the hash code H (M). The hash value is afix to the message at the source. The receiver authenticates the message by recalculating this hash value. The attributes can be used to generate the hash which can be preserved while scrambling the data. So, the hash calculated using the plaintext data and the encrypted data will remain the same. We proposed combine framework where the parameterized hash value of an encrypted image is designed to be the similar as the hash value of the parent unencrypted original image. 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. We also present the chaos based encryption that employed on the data points to scramble the information. We have also done the image comparison for an input image and decrypted image and we observed that PSNR value is + Inf dB. A lower value for MSE means lesser error logically, a higher value of PSNR is good because it means, values for PSNR range between infinity for identical images. It means there is no loss in images as results shown in Table 4.2. Comparison Table 4.1 represents the difference between the watermarking and secure message authentication. We can see that there output image PSNR is +Inf dB means image is identical and where as in watermarking decrypted image there is lossy image.

(a) Original Leena Image b) Encrypted Leena image

Fig 4.1: (a) Original image and (b) Encrypted image.

Table 4.1 Comparison Secure message authentication and Joint asymmetric Watermarking based on lena image.

Feature	**PSNR (A Joint asymmetric watermarking)**	**PSNR Secure Message Authentication)**
Original	-	-
Encryption	+59.53 dB	+63.47 dB
Decryption	+ 36.071 dB	+ Inf dB

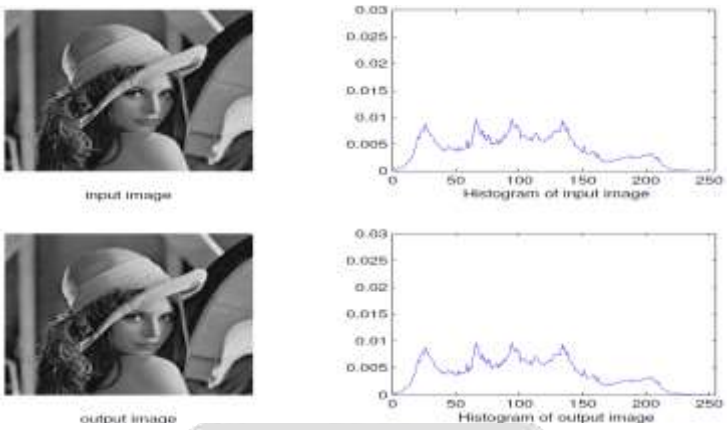

Fig 4.2: Comparing input & output Leena image with the help of histogram.

Table 4.2 Detection Performance for Leena image

Feature	PSNR
Original	-
Encryption	+63.47 dB
Decryption	+ Inf dB

For each image, firstly we compute the 16 × 16 block DCT coefficients. After that each block is encrypted. Chaos encryption based on Cat map has been employed. The key 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 and q are decided by the key but we also have randomized the number of iterations for the Cat map. Our 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 is of 100 bits length. They are shown in the form of images of dimension 10×10. The Results the validity of the proposed algorithm. The hash of the original image and the encrypted image are same.

5. CONCLUSION

We proposed combine framework where the parameterized hash value of an encrypted image is designed to be the similar as the hash value of the parent unencrypted original image. By allowing a portion of the statistical signature in the original image, it becomes possible to validate the authenticity of the encrypted image without tapping into its contents. Here we have observed that the mean and variances of the blocks remain the same even after encryption. Formulates the problem of authenticating encrypted data, and discussed about the invariant watermark, invariant hashes and the zero-knowledge authentication. We also present the chaos based encryption that employed on the data points to scramble the information. We then recommend and analyze the novel method for calculating the hash used these two features to construct the hash value. This simple choice of features also depicts a significant variability across a variety of images. The aim of the project work will be to formulate the problem of authenticating encrypted information and design of a non-complicated and light weight hashing algorithmic rule applicable to encrypted images. By allowing a segment of the statistical signature in the original image, it becomes potential to validate the authenticity of the encrypted image without tapping into its contents.

6. REFERENCES

[1] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, Oct 1949.

[2] I. Pitas, "A Method For Signature Casting On Digital Images", Proceedings., International Conference on 1996.

[3] Yuliang Zheng, "Digital Signcryption or How to Achieve Cost", CRYPTO, 1997.
[4] Mitchell et. al, "Robust Audio Watermarking Using Perceptual Masking, Signal Processing" , pp. 337-355 (1998)
[5] J. Cox, M. L. Miller, and J. A. Bloom, "Watermarking applications and their properties," in *Proc. Int. Conf. on Information Technology: Coding and Computing*, pp. 6–10, March 2000.
[6] E. T. Lin, C. I. Podilchuk, and E. J. Delp, "Detection of image alterations using semi-fragile watermarks," in *SPIE Intl. Conf. on Security and Watermarking of Multimedia Contents II*, Jan 2000.
[7] H. Cheng and X. Li, "Partial Encryption of Compressed Images and Videos," *IEEE Transactions on Signal Processing*, vol. 48, no. 8, pp. 2439–2451, 2000.
[8] Jiri Fridrich and Miroslav Goljan SUNY Binghamton, Binghamton, "Robust Hash Functions for Digital Watermarking" IEEE, Proceedings in Information Technology: International Conference on Coding and Computing, 2000. Publication Year: 2000 , pp. 178 – 183.
[9] Mihir Bellare, Chanathip Namprempre, "Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm", Advances in Cryptology, ASIACRYPT 2000, Volume 1976 of Lecture Notes in Computer Science, pp. 531-545, 2000.
[10] Hugo Krawczyk, "The Order of Encryption and Authentication for Protecting Communications", Proceeding CRYPTO '01 Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology pp. 310 – 331, 2001.
[11] Charanjit S. Jutla, "Encryption Modes with Almost Free Message Integrity", Proceeding EUROCRYPT '01 Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology
pp. 529 – 544, 2001.
[12] Ton Kalker, Jaap Haitsma, Job Oostveen, "Issues with Digital Watermarking and Perceptual Hashing",12 November 2001, ISBN: 9780819442420.
[13] John Black, Hector Urtubia, "Side-Channel Attacks on Symmetric Encryption Schemes: The Case for Authenticated Encryption", Proceeding Proceedings of the 11th USENIX Security Symposium pp. 327 – 338.
[14] Jee Hea An, Yevgeniy Dodis, Tal Rabin, "On the Security of Joint Signature and Encryption", Proceeding EUROCRYPT '02 Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology pp. 83-107.
[15] Yevgeniy Dodis, "Concealment and its Applications to Authenticated Encryption", Proceeding EUROCRYPT'03 Proceedings of the 22nd international conference on Theory and applications of cryptographic techniques pp. 312-329.
[16] Hamza Ozer, Bulent Sankur, Nasir Memon, " Robust Audio Hashing for Audio Identification" Eusipco 2004, Conference European Association for Signal Processing (EURASIP), pp. 2091-2094.
[17] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", *Chaos, Solitons and Fractals, Elsevier*, pp. 749–761, 2004.
[18] Min-Shiang Hwang and Chi-Yu Liu, "Authenticated Encryption Schemes: Current Status and Key Issues", International Journal of Network Security, Vol.1, No.2, pp. 61–73, Sep. 2005.
[19] S.Lian, Z. Liu, R. Zhen, and H. Wang, "Commutative Watermarking and Encryption for Media Data", *OE Lettters, SPIE*, vol. 45(8), 2006.
[20] Qiming Li, Nasir Memon, Husrev T. Sencar, "Security Issues in Watermarking Applications A Deeper Look", In *ACM Workshop on Multimedia Content Protection and Security*, Santa Barbara, CA, October 2006.
[21] G. Boato, V. Conotter, F. G. B. D. Natale, and C. Fontanari, "A joint asymmetric watermarking and image encryption scheme," in *Proceedings of SPIE Electronic Imaging*, vol. 6819, pp. 601–602, 2008.
[22] 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.
[23] S. Lian, "Quasi Commutative Watermarking and Encryption for Secure Media Content Distribution," *Multimedia Tools Appl, Springer*, vol. 43, pp. 91–107, 2009.
[24] Kashyap, S.; Karthik, K., "**Authenticating Encrypted Data"** Communications (NCC), National Conference on 2011 Year: 2011 , pp. 1 – 5.