International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958, Volume-2, Issue-2, December 2012

Secure Message Authentication

Jyoti R. Rajput, Kalyankar Pravin P.

Abstract— Digital watermarks have recently been proposed for authentication of both video data and still images and for integrity verification of visual multimedia. In such applications, the watermark has to depend on the original image. It is important that the dependence on the key be sensitive, while the dependence on the image be continuous (robust). The proposed system basically uses authentication and encryption mechanism that are two intertwined technologies that help to insure that your data remains secure.* Authentication *is the process of insuring that both ends of the connection are in fact who they say they are. This applies not only to the entity trying to access a service (such as an end user) but to the entity providing the service, as well (such as a file server or Web site).* Encryption *helps to insure that the information within a session is not compromised. This includes not only reading the information within a data stream, but altering it, as well. While authentication and encryption each has its own responsibilities in securing a communication session, maximum protection can only be achieved when the two are combined. For this reason, many security protocols contain both authentication and encryption specifications.

Index Terms— Encryption, Authentication, DCT cryptographic security, Hash Function.

I. INTRODUCTION

Hash functions are frequently called message digest functions. Their purpose is to extract a fixed length bit string From a message (computer file or image) of any length. Obviously a message digest function is a many to-one mapping. In cryptography, hash functions are typically used for digital signatures to authenticate the message being sent so that

The recipient can verify that the message is authentic and that it came from the right person. The requirements for a cryptographic hash function are [1]

- Given a message m and a hash function H, it should be easy and fast to compute the hash h=H(m)
- Given h, it is hard to compute m such that h=H(m) (i.e., the hash function should be one way)
- Given m, it is hard to find another message m such that H(m')=H(m) (property of being collision free)

From the above properties it is clear that hash functions are "infinitely" sensitive in the sense that a small perturbation of the message *m* will give you a completely different bit-string *h*. In applications involving digital watermarking and authentication of digital images, the requirements on what should be a digest of an image are somewhat different. Changing the value of one pixel does not make the image different or non-trustable. One can say that we want approximately the same hash bit-strings for two images whenever the human eye can say that these two images "are the same".

Manuscript received on December, 2012.

Jyoti R Rajput, Department Computer Science and Engineering, BAMU/ COE Osmanabad/ Organization TPCT's, City Osmanabad, Country India.

Kalyankar Pravin P.,Department Computer Science Engineering, BAMU/ COE Osmanabad/ Organization TPCT's, City Osmanabad, Country India.

Obviously, this is a challenging problem that can never be solved to our complete satisfaction. This is because the fuzzy concept of two images being visually the same is inherently ill defined and difficult, if not impossible, to grasp analytically. For example, changing one pixel in the pupils of a person's eye is for all purposes a negligible change. But once we change the color of every pixel in the pupil from, say, blue to brown, an important personal characteristic has been changed. Thus, we would conclude that the two images are no longer the same. However, the pupils can occupy a very small part of the image and our robust hash, not knowing the importance of eyes, may return the same hash bit-string. Being aware of these and other limitations, nevertheless, in this paper, we attempt to meaningfully define the concept of a robust visual hash. Before we start with the definition and ideas how to construct such a function, we give a brief introduction into oblivious digital watermarking and explain how robust hash will play an important role in specific watermarking applications, such as authentication and fingerprinting [2].

II. DIGITAL WATERMARKING

A watermark of a digital image is a pseudorandom bit sequence added to an image. It is known only to the owner of that image so that others can not duplicate or remove it. Therefore it can serve as "proof" that the owner really owns this image. There should be no perceptual degradation of the image, and the watermark should be detectable even after manipulation of the image. There are two main models for digital image watermarks[3]:

1. The owner of the image stores some information about every image that he publishes. This information is needed for verification of the watermark bit sequence.
2. There is no extra information available except the watermark information added to the image.

Obviously, the second model is more difficult to realize, since the user of the image can always try to destroy the complete watermark information by manipulating the image. In this paper, we use a slightly modified approach which needs very little extra information. This information can be shared between different images. The owner of the copyright as to remember a password used in the watermarking algorithm to check whether a watermark is embedded inside an image or not.

The general procedure for embedding the watermark information into the image is as follows:

We transform the image using the well known Discrete Cosine Transform (DCT), then we add the watermark to selected coefficients of the transformed image, and finally we invert the DCT to get an image very similar to the original one with included watermark. The detection procedure starts by first transforming the input image with DCT and then tries to extract the watermark information from some selected coefficients. In our algorithm, we use a cryptographic hash function to determine which of the coefficients of the result of the DCT transform are used for embedding the watermark information.

- **Watermarking Embedding Process**

The algorithm which embeds the watermark in the text is called embedding algorithm. The inputs for embedding algorithm are combined image and text watermark and the text document. The embedding algorithm performs pre processing of image and the text to convert the watermarks pure alphabetical in nature.

Inputs are combined image and text watermark and text document. Split the combined watermark into text and image watermarks. Preprocess text watermark which includes, discarding white spaces, special characters, digits etc to make the watermark pure alphabetical. Pre process image which converts image to gray scale and scaling to standard size(100 x 100 pixels).Convert image to plain text by normalization process.

The two textual watermarks (watermarks obtained after text pre-processing and image pre processing) an partial key containing a partition size (Pr) and group size (GS) is given as input to the embedding algorithm. The embedding algorithm generates the watermark key using the inherent properties of text. Encrypt the text document using RSA encryption algorithm to increase security of text which is presented below.

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 P_W then mathematically[4],

$E(Wembed(P,W,Kw),K) = E(Pw,K) = Pw,encrypt$ (1)

We want the watermark to remain invariant to the encryption process. That is to say, we want a scheme wherein we can extract the watermark without decrypting the received data.

Mathematically,

$Wextract(Pw,encrypt,Kw) = W$ (2)

III. METHODOLOGY

The proposed project work highlights a novel approach of authenticating an encrypted data using both user-defined secret key and hash function generated in image format. The proposed system basically uses authentication and encryption mechanism that are two intertwined technologies that help to insure that your data remains secure[11][12]. Authentication is the process of insuring that both ends of the connection are in fact who they say they are. This applies not only to the entity trying to access a service (such as an end user) but to the entity providing the service, as well (such as a file server or Web site). Encryption helps to insure that the information within a session is not compromised. This includes not only reading the information within a data stream, but altering it, as well. While authentication and encryption each has its own responsibilities in securing a communication session, maximum protection can only be achieved when the two are combined. For this reason, many security protocols contain both authentication and encryption specifications[12][13].

In the concept of networking and data security, often when two parties communicate over a network, they have two main security goals: privacy and authentication. In fact, there is compelling evidence that one should never use encryption without also providing authentication. Many solutions for the privacy and authentication problems have existed for decades, and the traditional approach to solving both simultaneously has been to combine them in a straightforward manner using so-called "generic composition." However, recently there have been a number of new constructions which achieve both privacy and authenticity simultaneously, often much faster than any solution which uses generic composition. In this proposed project, a secure approach is mechanized for ensuring both privacy and authenticity, the so-called "Authenticated Encryption" problem[11][13]. The proposed system has estimates the hash value of the data for which the encrypted process remains transparent to the hash function. The remaining part of the seminar document will briefly introduce the drawback of the existing we describe a previously proposed mechanism for robust extraction of bits from image blocks so that all similarly looking blocks, whether they are watermarked, unwatermarked or attacked by gray scale modifications, will produce almost the same bit sequence of a specified length N. We present some new results concerning the robustness of the hash bits with respect to intentional attempts to modify the hash. system, significance, problem statement, objectives, and methodology of the proposed project[13][12].

We describe a previously proposed mechanism for robust extraction of bits from image blocks so that all similarly looking blocks, whether they are watermarked, unwatermarked or attacked by gray scale modifications, will produce almost the same bit sequence of a specified length *N*. We present some new results concerning the robustness of the hash bits with respect to intentional attempts to modify the hash. The method is based on the observation that if a low frequency DCT coefficient of an image is small in absolute value, it cannot be made large without causing visible changes to the image. Similarly, if the absolute value of a low-frequency coefficient is large, we cannot change it to a small value without influencing the image significantly. To make the procedure dependent on a key, the DCT modes are replaced with low frequency, DC-free, (i.e., having zero mean) random smooth patterns generated from a secret key (with DCT coefficients equivalent to projections onto the patterns).For each image, a threshold Th is calculated so that on average 50% of projections have absolute value larger than Th and 50% are in absolute value less than Th.

This maximizes the information content of the extracted *N* bits. Using a secret key *K* (a number uniquely associated with an author, movie distributor, or a digital camera)we generate *N* random matrices with entries uniformly distributed in the interval [0, 1]. Then, a low-pass filter is repeatedly applied to each random matrix to obtain *N* random smooth patterns $P(i)$, $1 \square i \square N$. All patterns are then made DC-free by subtracting the mean from each pattern. Considering the block and the pattern as vectors, the image *I* is projected on each pattern $P(i)$, $1 \square i \square N$, and its absolute value is compared with the threshold *Th* to obtain *N* bits *bi*

if $|B \square P(i)| < Th$ $bi = 0$

if $|B \square P(i)| \square Th$ $bi = 1$.

Since the patterns $P(i)$ have a zero mean, the projections do not depend on the mean gray value of the block and only depend on the variations within the block itself. The distribution of the projections is image dependent and should be adjusted accordingly so that approximately half of the bits *bi* are zeros and half are ones. This will guarantee the highest information content of the extracted *N*-tuple. This adaptive choice of the threshold becomes important for those image operations that significantly change the distribution of projections, such as contrast adjustment or gamma Correction.Strong encryption provides a powerful mechanism that can be applied to many parts of an organization's data security practices, offering effective,

continuous protection of data. This protection can encompass a range of uses, from end-point devices in the field to the core of the central servers where vital information resides.

Hence reading the above comments about significance of data encryption, the proposed system furnishes following uniqueness that can be considered as importance of the topic:

- The proposed project is much advanced than Steganographic technique. Steganographic techniques uses data embedded inside image using either public or private key. But the proposed system will not only user user-defined public key, but also it will deploy hash function in image format that is quite impossible to break.
- The proposed project is highly flexible and secure version of conventional cryptographic technique where they (conventional techniques) needs to manage a massive key management protocols. The proposed system is light weight as the hash value extracted from image file is only 100 bits in size.
- The mechanism of the proposed system is quite unique compared to conventional system. The proposed system performs encryption on each block of images (16x16 block) using Discrete Cosine Transform. The technique is highly robust and renders almost impossible for any attacker to perform decryption.

IV. RESULT

To, show the expected results it is tested across a variety of images for two reasons:

- The hash value should be unique to a given image. Because 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.
- 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 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 .
- We also verify that the hash for each image obtained from the proposed algorithm is unique.
- The hashes obtained from the proposed algorithm. These hashes remain transparent to the encryption process. To verify experimentally by finding out the hash of the original image and the encrypted image. Also, the hashes obtained from two different encrypted versions (same encryption algorithm but different keys used) of the same original image remain equal.

V. CONCLUSION

In this paper, we introduce the concept of a hash function with applications to digital image watermarking for authentication and integrity verification of video data

and still images. The robust image digest can also be used as a search index for efficient database searches. The hash function depends on a parameter K (a secret key) in a sensitive manner and on the image in a robust manner. Conventionally message authentication codes and also the method of encoding are treated as vertical security method, wherever message authentication codes are deployed to confirm knowledge credibility whereas encoding is employed to preserve confidentiality. During this proposed project work, a framework is introduced that uses hash value of an encrypted image that is intended to be identical because the hash value of the parent unencrypted original image. Since the hash price is computed while not decrypting the initial knowledge, one will prove credibility while not truly revealing the knowledge. The prime intention 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. We plan to use these two features to construct the hash value. We may make further additions if time permits.

REFERENCES

[1] B. Schneier, Applied Cryptography, John Wiley&Sons, New York, 1996.
[2] Robust Hash Functions for Digital Watermarking Jiri Frindrich and Miroslav Goljan
[3] Digital Image Watermarking Using The Discrete Cosine Transform And The MD5 Cryptographic Hash Function Wahyu Prakosa Adi & Volker Müller Duta Wacana Christian University
[4] Kashyap, S.; Karthik, K. Authenticating Encrypted Data Communications (NCC), National Conference on 2011 Year: 2011, Page(s): 1 – 5
[5] J. Cox, M. L. Miller, and J. A. Bloom, "Watermarkingapplications and their properties," in Proc. Int.Conf. on Information Technology: Coding an 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] S. Lian, "Quasi Commutative Watermarking and Encryption for Secure Media Content Distribution," Multimedia Tools Appl, Springer, vol. 43, pp. 91–107, 2009.
[9] S.Lian, Z. Liu, R. Zhen, and H. Wang, "Commutative Watermarking and Encryption for Media Data," OE Lettters, SPIE, vol. 45(8), 2006.
[10] 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.
[11] C. E. Shannon, "Communication Theory of Secrecy Systems," Bell System Technical Journal, vol. 28, pp. 656–715, Oct 1949.
[12] 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.
[13] Z. Lv, L. Zhang, and J. Guo, "A Symmetric Image Encryption Scheme Based on Composite Chaotic Dispersed DynamicsSystem," Proc. Of Second Symposium on Computer Science and Computational Technology, pp. 191–194, 2009
[14] Hugo Krawczyk, The Order of Encryption and Authentication for Protecting Communications (Or: How Secure is SSL?)?, Proceeding CRYPTO '01 Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology Pages 310 – 331, 2001
[15] 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 Pages 529 – 544, 2001

[16] Phillip Rogaway, Mihir Bellare, John Black, OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption, ACM Journal Name, Vol. V, No. N, M 2003, Pages 1–3

[17] Yuliang Zheng, Digital Signcryption or How to Acheieve Cost (Signature & Encryption)<<Cost(Signature)+Cost(Encryption), CRYPTO, 1999

[18] 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

[19] Ton Kalker, Jaap Haitsma, Job Oostveen, Issues with Digital Watermarking and Perceptual Hashing, Date: 12 November 2001, ISBN: 9780819442420

In 2006, Jyoti R Rajput received a Bachelor degree from the Information Technology of Visvesvaraya Technological University, Belgaum, currently works as Asst. Prof. And also student in Master Program of the faculty of Computer Science and Engineering College of Engineering Osmanabad, BAMU University, Aurangabad, Maharashtra, India. Presented many papers in national Conferences.

Prof .Kalyankar P.P received his Bachelor degree in Computer science & Engineering from Walchand Institute of Technology, Solapur, Shivaji University, Kolhapur. He has completed ME(CSE) from Walchand College of Engineering, Sangli, Shivaji University Kolhapur. His work has been published in various National and International Conference and various International Journal. Presently he is working at TPCT College of Engineering, Osmanabad, BAMU University, Aurangabad, Maharashtra, India.He is Associate Professor and Recognized as PG Teacher and Guide. He is holding the position of HOD of MCA Department. He has attended various AICTE approved Conferences and workshops. He is member of various professional bodies like IE, ISTE. He is pursing for Ph.D.