Suresh Gyan Vihar University,
Jaipur International Journal of Converging Technologies and Management (IJCTM)
Volume 2, Issue 1, 2016
ISSN: 2455-7528

"Image Authentication & Watermarking Using Message Digest"

Gajanand Sharma[1] Prof (Dr.) Dinesh Goyal[2]
[1]Ph.D Scholar [2]Principal-GVSET
SGV University, Jaipur SGV University, Jaipur
gajanan.sharma@gmail.com, dinesh8dg@gmail.com

ABSTRACT: Watermarking is a promising solution to protect the copyright of multimedia data through Transcending, because the embedded message is always included in the data. Because of the fidelity constraint, watermarks can only be embedded in a limited space in the multimedia data.

As a side effect of these different requirements, a watermarking system will often trade capacity and perhaps even some security for additional robustness. Watermarking techniques can be classified into two types Spatial and frequency Domain.

In this work proposed to design a new watermarking technique in which Message Digest of an Image will be calculated & then it is embedded into the Image using LSB technique. So the Message Digest of an Image will act is its own watermark. This it creates two tier of security.

1. INTRODUCTION: With the speedy development and extensive use of Internet, information communication faces a huge challenge of protection. We require a protected and safe way to convey information. Encryption is a widespread system that is used for encrypting information. Except this for one it is very easy to gain the interest of the attackers because the message cannot be understood directly. The information can be captured, interpreted and yet spread after damage; hence, the reliability of the information is ruined. Prohibited copying, transforming, altering and copyright security have become very vital concerns with the hasty use of internet [1]. Hence, there is a burly need of expanding the techniques to fight all these problems. Digital watermarking [2] come into view as a solution for shielding the multimedia data. Digital Watermarking is the method of hiding or embedding an undetectable data into the given data. This undetectable data is called watermark or metadata and the given data is called cover data. There has been development of high speed computer networks in terms of Internet over last decades. Internet provides the means of new business, new techniques, leisure, and collective opportunities in the form of electronic publishing and advertising, real-time information release, invention ordering, operation Processing, digital repositories and libraries, web epapers and magazines, network video and audio, personal communication, lots more. The new opportunities can be broadly grouped under the label "electronic commerce". The expenditure effectiveness of selling software, high class art work in the form of digital images and video sequence by communication over World Wide Web (www) is greatly enhanced consequent to the improvement of technology. Sending hard copies by post is now a thing of past. However the industrial exploitation of the www is gradually being more acceptable, Anxiety on the security part of the trade has only channeled the operation to be restricted to the transmission of demo and free versions of software. Paradoxically, the cause for the growth is also of the apprehensive about the use of digital formatted data.

1.1 Watermarking: Watermarking embeds identifying information in an image, which is not always hidden in such a manner it cannot easily be removed. It can also contain device control code that prevents illegal recording. Another application of watermarking is copyright control, in which an image owner seeks to prevent illegal copying of the image. Watermarking is a promising solution to protect the copyright of multimedia data through Transcending, because the embedded message is always included in the data. Because of the fidelity constraint, watermarks can only be embedded in a limited space in the multimedia data. There is no evidence that watermarking techniques can achieve the ultimate goal to retrieve the right owner information from the received data after all kinds of content-preserving manipulations [4].

1.2 Watermarking Process: A watermarking system is made up of a watermark embedding system and a watermark recovery system. The system also has a **key** which could be either a public or a secret key. The **key** is used to enforce security, which is prevention of unauthorized parties from manipulating or recovering the watermark.

The inputs during the encoding process are the original data, the cover object and the output is the recovered watermarked data W.

The digital watermark embedding and retrieval is as shown in the figure 2.9 and figure 2.10**[9].** In the embedding process, the watermark to be embedded is hidden in the

Suresh Gyan Vihar University,
Jaipur International Journal of Converging Technologies and Management (IJCTM)
Volume 2, Issue 1, 2016
ISSN: 2455-7528

cover object, may be an image, audio or video file and during extraction, watermark is retrieved and removed from the image to obtain the original image.

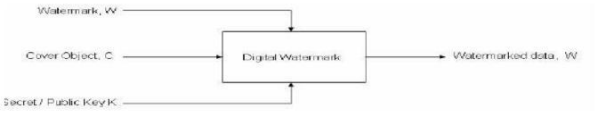


Fig.1: Watermark Embedding [9]

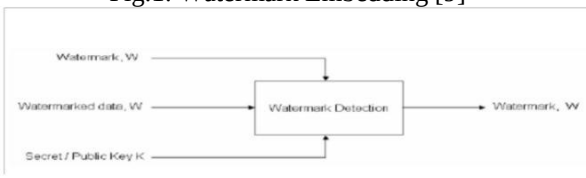


Fig.2: Watermark Detection [9]

1.3 **Message Digest:** MD5 is the safest one in a series of message digest algorithms designed by Professor Ronald Rivest of MIT (Rivest, 1992). When investigative work indicated that MD5's predecessor MD4 was probably to self-doubt, MD5 was designed in 1991 to be a secure alternate for the same.

MD5 processes a variable-length message into an output of fixed-length i.e. 128 bits. The input message is broken up into chunks of the blocks of 512 bits (sixteen 32-bit words); the message is padded so that its length is divisible by 512. The padding works as follows: first a single bit, 1, is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits less than the multiple of 512. The remaining bits are filled up with 64 bits representing the length of the original message, modulo 2^{64}.

Message Digest 5: The MD5 function is a cryptographic algorithm that takes an input of arbitrary length and produces a message digest that is 128 bits long. The digest is sometimes also called the "hash" or "fingerprint" of the input. MD5 is used in many situations where a potentially long message needs to be processed and/or compared quickly. The most common application is the creation and verification of digital signatures.

How MD5 works

Preparing the input: The MD5 algorithm first divides the input in blocks of 512 bits each. 64 Bits are inserted at the end of the last block. These 64 bits are used to record the length of the original input. If the last block is less than 512 bits, some extra bits are 'padded' to the end.

MD5 helper functions:

The buffer: MD5 uses a buffer that is made up of four words that are each 32 bits long. These words are called A, B, C and D. They are initialized as word A: 01 23 45 67 word B: 89 ab cd ef word C: fe dc ba 98 word D: 76 54 32 10

The table: MD5 further uses a table K that has 64 elements. Element number i is indicated as Ki. The table is computed beforehand to speed up the computations. The elements are computed using the mathematical sin function:

Ki = abs(sin(i + 1)) * 232 ***Four auxiliary functions:*** In addition MD5 uses four auxiliary functions that each take as input three 32-bit words and produce as output one 32-bit word. They apply the logical operators and, or, not and xor to the input bits.

F(X,Y,Z) = (X and Y) or (not(X) and Z)
G(X,Y,Z) = (X and Z) or (Y and not(Z))
H(X,Y,Z) = X xor Y xor Z
I(X,Y,Z) = Y xor (X or not(Z))

Processing the blocks: The contents of the four buffers (A, B, C and D) are now mixed with the words of the input, using the four auxiliary functions (F, G, H and I). There are four rounds, each involves 16 basic operations. One operation is illustrated in the below figure

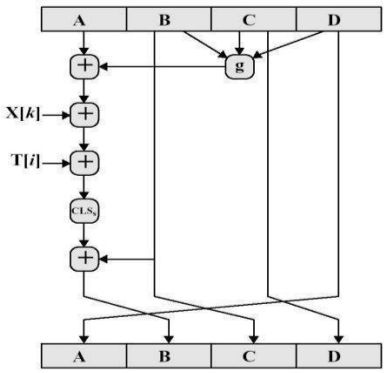


Fig.3: Operation of block

The output: After all rounds have been performed, the buffers A, B, C and D contain the MD5 digest of the original input.

2. PROBLEM DOMAIN: Security has become an indivisible matter as information technology is ruling the world now. Cryptography is the learning of mathematical methods related phases of Information Security such as data security, confidentiality, entity validation and data origin authentication, but it is not the only means of

Suresh Gyan Vihar University,
Jaipur International Journal of Converging Technologies and Management (IJCTM)
Volume 2, Issue 1, 2016
ISSN: 2455-7528

providing information security, rather techniques.

However in recent years digital Steganography has started itself as a significant discipline That is due in part to the strong interest. Unfortunately, given the high volume of the introduced techniques, the literature lacks a comprehensive review of these methods. All the existing processes of watermarking focus on the embedding strategy and give no deliberation to the dual authentication or copyright protection.

Many of the proposed methods take for granted flexibility to noise, double compression, and other image processing manipulations are not required in the Steganography context. As such, in the warden passive attack scenario their hidden data will be destroyed or will not be retrievable.

Adaptive Watermarking intended at identifying textural or quasi-textural areas for embedding the secret data runs into a few problems at the decoder side since its classification algorithms are not salient. In this thesis, skin-tone areas are the preferred choice for texture detection since the detection algorithm is robust and unique.

In most of the watermarking Techniques the watermark is an external component, here we try to generate watermark from the Image itself. Normally Message Digest works on text only. MD has not been used for images for long also the technique of automatic Watermark generation has not been used for long that too an encrypted one.

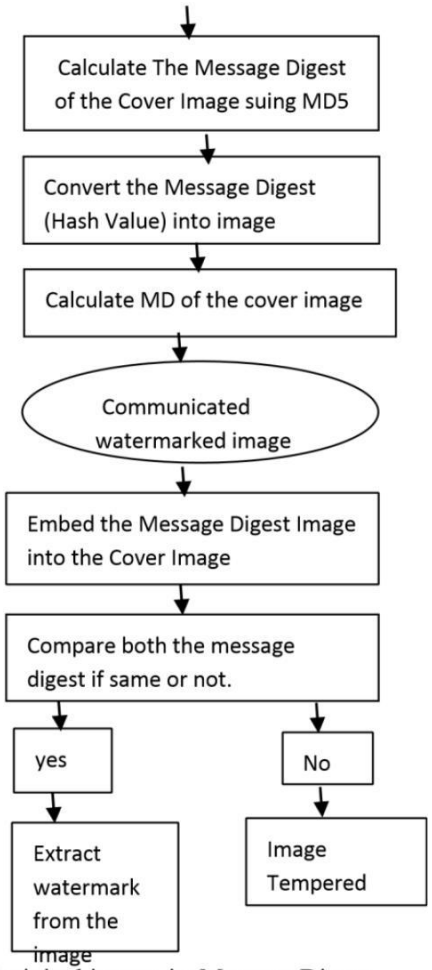
2.1Proposed Work: As discussed in our first chapter and motivation generated from review literature we find that many techniques exist for watermarking an image using either text, image or any other media as the watermark is embedded in the cover image. There are also many techniques of watermarking involving, Least Significant bit, Discrete Wavelet
Transformation, Discrete cosine Transformation and many more, which effectively and more importantly they ensure and protected communication of the cover object which delivers the result of watermarking to the receiver with minimum redundancy.

One of the arts of watermarking for copyright protection is Cover Generation Technique, in this technique the message which user wants to send the end user converts itself into the image and then the receiver cracks the image to obtain the secret message hidden inside.

one of the Here in this dissertation we propose an art of message Generation technique, in which the Cover image is used to create the secret message and then that secret message is embedded into the cover image. For implementing the image-based same the Message Digest using MD5 algorithm is calculated of the cover image, which is converted into a in signal processing. image then this MD5 image is embedded into cover image using 1 LSB(Least Significant Bit).

Our work comprise of two stages: **Stage 1:** It is done at the sender end; the sender calculates the Message Digest using MD5 algorithm of the cover image, which is converted into a image then this MD5 image is embedded into cover image using 1 LSB (Least Significant Bit). The flow chart that at the sender end is as follows:

Stage 2: It is done at the receiver end; the receiver decomposes the watermarked image and extracts the hash image and finds the hash value of cover image and compares both of them



The snapshots of original image, its Message Digest, Embedded Image and recovered watermark image are

Suresh Gyan Vihar University,
Jaipur International Journal of Converging Technologies and Management (IJCTM)
Volume 2, Issue 1, 2016
ISSN: 2455-7528

as follows:

Fig.4: Birds

Fig.5: Building

Fig.6: Horses

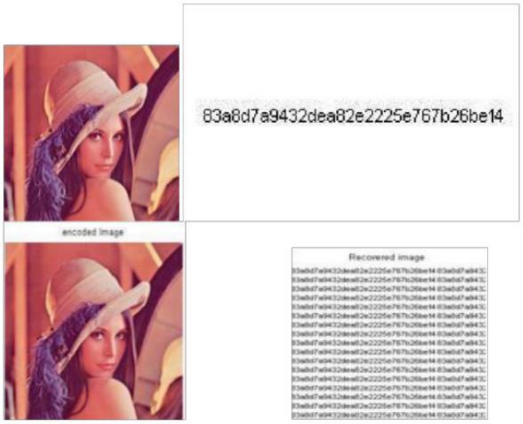


Fig.7: Lena

Fig.8: Walking

Fig.9: Logo

Suresh Gyan Vihar University,
Jaipur International Journal of Converging Technologies and Management (IJCTM)
Volume 2, Issue 1, 2016
ISSN: 2455-7528

After performing all the experiments it is time to do the analysis of the results obtained of the outcome of the same.

We analyze the outcome of efforts made by the sender and results of watermarked image

Table1: PSNR of Original Image compared with Watermarked Image

4.FUTURE WORK: In future one can perform the further task to enhance better results and good security:

1. Use embedding techniques like DCT or DWT
2. Use various kind of images formats.
3. Use other multimedia formats like moving images & video.
4. Use other types of Message digest for high quality authentication.
5. Use encryption techniques in tandom to the above work for better security too.

REFERENCES:

[1]. Mrs. A.Angel Freeda, M.Sindhuja, K.Sujitha, "Image Captcha Based Authentication Using Visual Cryptography", IJREAT, ISSN: 2320 – 8791, April 2013

[2]. Mr. A.Duraisamy, Mr.M.Sathiyamoorthy, Mr.S.Chandrasekar, "Protection of Privacy in Visual Cryptography Scheme Using Error Diffusion Technique Using Error Diffusion Technique", IJCSN ISSN (Online) : 2277-5420 April 2013

[3]. Ankita Gharat, Preeti Tambre, Yogini Thakare,

Suresh Gyan Vihar University,
Jaipur International Journal of Converging Technologies and Management (IJCTM)
Volume 2, Issue 1, 2016
ISSN: 2455-7528

S. No.	Name of Image	Size of Image	PSNR
1	Bird	300 X 300	55.4940
2	Building	300 X 300	55.7559
3	Lena	512 X 512	55.9603
4	Walking	204 X 204	55.9360
5	Logo	60 X 60	55.6201
6	Horses	225 X 225	55.3104

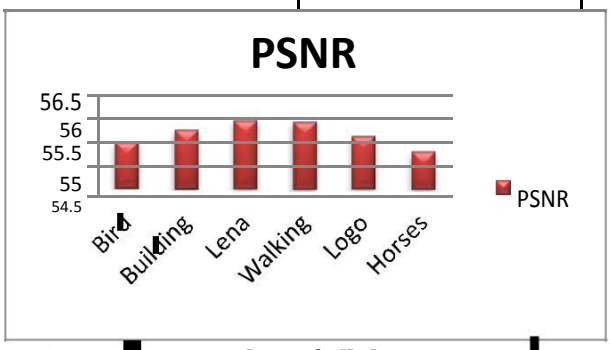


Fig. 10 : PSNR Values of all the test images

3. CONCLUSION: There are also many techniques of watermarking involving, Least Significant bit, Discrete Wavelet Transformation, Discrete cosine Transformation and many more, which effectively and more importantly they ensure and protected communication of the cover object which delivers the result of watermarking to the receiver with minimum redundancy.

One of the arts of watermarking for copyright protection is Cover Generation Technique, in this technique the message which user wants to send the end user converts itself into the image and then the receiver cracks the image to obtain the secret message hidden inside.

Here in this dissertation we proposed an art of message Generation technique, in which the Cover image is used to create the secret message and then that secret message is embedded into the cover image. As our results show that the PSNR of final output watermarked image is very good in terms of input image and the work done for securing the image for communication has also been achieved. We also achieved the goal of ensuring authentication of the watermark image by verifying the Message Digest.

Prof. S.M. Sangave "Biometric Privacy Using Visual Cryptography" IJARCET, ISSN: 2278 – 1323, January 2013

[4]. Vilma Petrauskiene, Rita Palivonaite, Algiment Aleksa, Minvydas Ragulskis "Dynamic visual cryptography based on chaotic oscillations", ELSEVIER, 2013.

[5]. Md. Tanbin Islam Siyam, Kazi Md. Rokibul Alam and Tanveer Al Jami, "An Exploitation of Visual Cryptography to Ensure Enhanced Security in Several Applications", IJCA ISSN: 0975 – 8887, 2013

[6]. Anushree Suklabaidya, "Visual Cryptographic Applications", IJCSE, ISSN: 0975- 3397, June 2013

[7]. M. L. Miller, I. J. Cox, and J. A. Bloom, "Informed embedding: exploiting image, Digital watermarking, Morgan Kaufmann Publishers Inc., San Francisco, CA, 2001.

[8]. Jitao Jiang, Xueqiu Zhou and Xiaohong Liu, "An improved algorithm based on LSB in digital image hidden", Journal of Shandong University of Technology (Science and Technology), vol. 20(3), 2006, pp. 66-68, ISSN: 1672-6197.0.200603-018.

[9]. Juan Zhou, Shijie Jia, "Design and Implementation of Image Hiding System Based on LSB", Computer Technology and Development, vol. 17 (05), 2007, pp. 114-116, doi: cnki: ISSN: 1673629X.0.2007-05-034.

[10]. Gil-Je Lee, Eun-Jun Yoon, Kee Weng Yoo "A new LSB based Digital Watermarking Scheme with Random Mapping" in 2008 International Symposium on Ubiquitous Multimedia Computing.

[11]. Jianwei Zhang, Xinxin Fang, Junhong Yan, "Implement Of Digital Image Watermarking LSB", Control & Automation, vol. 22(10), 2006, pp. 228-229, doi: cnki:ISSN:1008-0570.0.200610-083.

[12]. Qian-lan Deng Jia-jun Lin, "A Steganalysis of LSB based on Statistics", Modern Computer, No.1, 2006, pp. 46-48, doi: cnki: ISSN: 10071423.0.2006-01-010.

[13]. Jian-quan Xie, Chun-hua Yang. "Adaptive hiding method of large capacity information", Journal of computer applications, vol. 27(5), 2007, pp.10351037, doi: CNKI: ISSN: 10019081.0.2007-05-001.

[14]. Hongwei Lu, Baoping Wan, "Information Hiding Algorithm Using BMP Image", Journal of Wuhan University of Technology, vol.28(6), 2006,pp. 96-98, doi: cnki: ISSN: 16714431.0.2006-06-027.

[15]. P. Geum-Dal,; Y. Eun-Jun,; Y. Kee-Weng , (2008) "A New Copyright Protection Scheme with Visual Cryptography", Second International Conference on Future Generation Communication and Networking Symposia. pp. 60-63.

[16]. J.J. Eggers, J.K. Su and B. Girod, "A Blind Watermarking Scheme Based on Structured Codebooks," IEE Colloquium: secure image and image authentication, London, UK, April 2000

[17]. A. Westfield, A. Pfitzmann. "Attacks on steganographic systems". In Proceedings of 3rd. International Workshop Computer Science (IH '99) Germany, 1999.