International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 3, Issue 4, July-August 2014 **ISSN 2278-6856**

Authentication of digital image by the use of fragile watermarking

[1]Ms. Namrata V. Komte , [2]Prof. Ms. V. A. More
[1,2] Department of electronics engineering
MGM's Jawaharlal Nehru engineering college, N-6, cidco, Aurangabad

Abstract

Digital watermarking is used to hide the information inside a signal, which can not be easily extracted by the third party. Its widely used application is copyright protection of digital information. It is different from the encryption in the sense that it allows the user to access, view and interpret the signal but protect the ownership of the content. One of the current research areas is to protect digital watermark inside the information so that ownership of the information cannot be claimed by third party. With a lot of information available on various search engines, to protect the ownership of information is a crucial area of research. In latest years, several digital watermarking techniques are presented based on discrete cosine transform (DCT), discrete wavelets transform (DWT) and discrete fourier transforms (DFT). In this paper, we propose an algorithm for digital image watermarking technique based on singular value decomposition; both of the L and U components are explored for watermarking algorithm. This technique refers to the watermark embedding algorithm and watermark extracting algorithm. The experimental results prove that the quality of the watermarked image is excellent and there is strong resistant against many geometrical attacks.

Index Terms:-Digital image watermarking, watermark embedding algorithm, watermark extracting algorithm, security analysis

1. INTRODUCTION

Content alteration destroys the integrity and Authenticity of the image. For hard authentication technique, the modification of image contents and of the watermark is not the same. The verification process in a watermarking system should be able to detect and localize exactly where the contents are tampered. It also should authenticate the image if the alteration is only on the watermark, because the tampered watermark does not affect the authenticity of the image. To the best of our knowledge, all the hard authentication algorithms have the tamper localization capability, but do not have the capability of distinguishing these two alterations. As a result, attackers can make the particular image not pass the verification process by only tampering the watermark. Fragile watermarks are designed to protect the authenticity and integrity of digital images by detecting changes in an image [1-2]. Other than having the property of thwarting attacks for secure communication applications, fragile watermarking Schemes typically have the functionalities for image authentication and tamper localization [3-7]. However, the feature of distinguishing whether the tampering is on image contents or on embedded watermarks, which might be important to practical applications, has not been addressed in the literature. This task is called the tamper discrimination. Forexample, if only the watermark is modified, themverification algorithm should indicate that the image is authentic and can be used as desired rather than regarded it as a fake. This is possible in that the attacker can forger the digital media by tampering the embedded watermark only, not contents, so as to confuse the system and to make the image fail the verification process. To overcome this problem, we Propose a fragile watermarking scheme for image authentication and tamper discrimination. The Proposed scheme can point out whether the modification made to the image is on the contents, the embedded watermark, or both. If tampering is on the image contents, the watermark verification algorithm will return a difference image that displays the altered regions. If only the watermark is modified, the difference image will show isolated dots spread all over the image. When both are tampered, the above two phenomena will occur simultaneously. The above situation may occur in the real world. For instance, a car causing the traffic accident runs away. The surveillance system (with watermarking capability captures the car and its license plate. In the picture, it clearly indicates the plate number "F606 YVG" of that Car (Fig. 1 (a)). Thus this photo can be used as the hard evidence to act against the driver. However, that driver may utilize the following two means to evade the responsibility. (1) Modifying the plate number. For example, the plate number can be changed to "R237 JAD" (Fig. 1 (b)). Since the digital photo is watermarked, this alteration can be detected by the verification system (Fig. 1 (c) is the result by Wong's algorithm [3]). This shows that the plate number has been Tampered. (2) Altering the watermark. This modification (Fig.1 (d)) does not affect the visual effect of the digital Photo. The plate number is still showing the actual Car that causes the accident. This kind of tampering can be detected by Wong's algorithm [3], as shown
in Fig.1 (e).

(a)

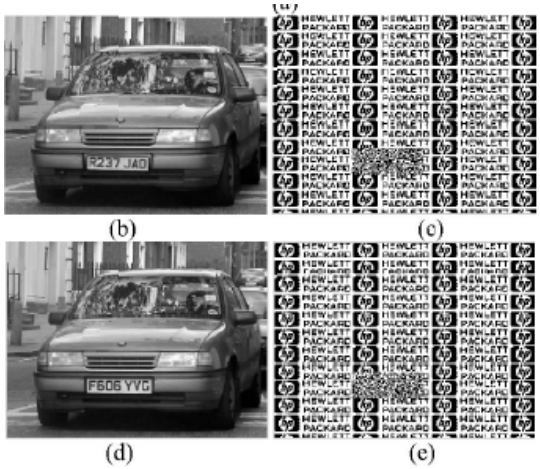


Fig. 1. Image authentication results by Wong's algorithm [3] (a) Original image, (b) plate number altered image, (c) verification result of (b), (d) image with only watermark being altered, (e) verification result of image (d)

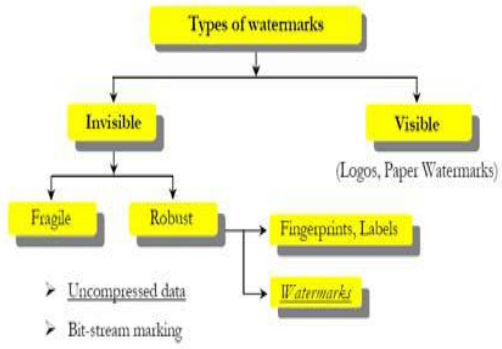
In the first case, the plate number of the picture is not the one in the accident. Obviously, it cannot be used as a proof. Thus the responsibility may be transferred to the third person. In the second case, the suspect may claim that the number has been altered and he/she is framed. Thus the suspect may be free of charge because this seemingly faked photo cannot be used as concrete evidence. To overcome the first problem, in addition to tamper localization, the watermarking algorithm should have the capability to recover the plate number of the tampered photo. Even though the plate number has been modified, the verification system is still able to show the actual plate number. Furthermore, if the watermarking algorithm is able to indicate that the modification of the digital image is made only on the watermark, and the content is genuine, then it resolves the second dilemma. As can be seen from Fig. 1, Wong's algorithm cannot distinguish the two situations mentioned above. Therefore, there is a need to develop a watermarking algorithm that not only have good tamper localization and security against attacks, but also have the ability to discriminate the watermark tampering from the content tampering.

2. WATERMARKING AND TYPES

2.1 WATERMAKING

Digitizing of multimedia data has enabled reliable, faster and efficient storage transfer and processing of data [1]. The ease with which the multimedia data can be utilized, amplifies possibilities to perform illegal copying and redistribution of the multimedia data. Multimedia data in the form of image, audio and video, can be easily manipulated and reproduced in digital domain using present day multimedia manipulation tools. There is great demand of techniques for handling the problems associated with the multimedia data. In this context, it is important to develop systems for copyright protection, protection against duplication, and authentication of content [2]. Techniques of data hiding specifically watermarking can be applied to protect multimedia data against these types of manipulations and duplications. Digital watermarking is a method to attest the owner identification of the multimedia data and discourage the unauthorized copying, by embedding perceptually transparent pattern in digital data by specially designed algorithms. Generally, a watermark represents the owner and the user's information which could be owner's logo or some control information suitable for embedding in the cover multimedia. Digital watermarking technology is now drawing the attention as a new method of protecting copyrights for digital images. It is realized by embedding data that is insensible for the human visual system. The embedded information data is called watermark. So watermarking in digital images is the process by which a discrete data stream is hidden within an image imposing imperceptible changes of the image. The root of watermarking as an information hiding technique can be traced in ancient Greece as Steganograpy, the science of watermarking is a modern subject was organized developed in recent years. Watermarking techniques are judged on the basis of their performance on a small set of properties. These properties include robustness, transparency, watermarking capacity, blind detection and security. Watermarking schemes are developed according to the requirements of the application and all applications do not require each of these properties in their entirety i. e. watermarking requirements are application dependent and some most desirable properties for these applications are conflicting in nature. Digital watermarking techniques are classified according to various criteria like robustness, perceptibility and embedding and retrieval methods. Robustness is an important criterion which means the ability of watermark to resist common image processing operations.

2.2. Types of watermark



2.2.1. Robust

Robust watermarking schemes are applied for proving ownership claims whereas fragile watermarking is applied to multimedia content authentication. These watermarking schemes have their own requirements in

terms of robustness. Robust watermarks should be able to survive a wide range of friendly operations and malicious attacks, whereas fragile watermarks are intolerable to both malicious and content preserving operations.

2.2.2. Fragile

Fragile watermarking techniques are designed with a goal to identify and report every possible tampered region in the watermarked digital media. Semi-fragile watermarks are intermediate in robustness between the two and are also used for image authentication. Some critical applications like medical imagining and forensic image archiving also requires the fragile watermarks to be reversible. The different quantitative parameters such as PSNR, True and false positive may be used for the evaluation of the method of watermarking schemes In recent years, the accessing of multimedia data or digital data has become very easy because of the fast development of the Internet. In other Words, this development makes unauthorized distribution of multimedia data. For the protection of multimedia data, a solution known as watermarking is used. After the approximate 20 years' research, different kinds of watermarking algorithm based on different theory concepts were introduced [1-3]. A digital watermark encodes the owner's license information and embeds it into data. Watermarking may be used to identify the image of owners' license information and to track illegal copies.

3. TECHNIQUES OF WATERMARKING

There are mainly two major techniques of watermarking

- Spatial domain: slightly modifies the pixels of one or two randomly selected subsets of an image
- Frequency domain: this technique is also called transform domain. Values of certain frequencies are altered from their original.

3.1. Spatial Domain

In this type of watermarking, the pixels of one or two randomly selected subsets of an image are modified. These modifications can even include the flipping of the low-order bit of each pixel. But this technique is not considered reliable for normal media operations like lossy compression or filtering.

- LSB Coding: The least significant bits of the host signals are modified by the watermark signal.
- Correlation Based: Pseudo random noise (PN) with a pattern W(x, y) is added to an image according to Patchwork

This algorithm has been proposed as an image watermarking scheme at the outset. This inserts the information into the time-domain signal. Original patchwork algorithm is refreshingly novel among many watermarking methods. Moreover, the population of each subset was very large: It was not adaptive to the signal: it added or subtracted constant d independently of the signal strength. Nonetheless, it has provided a solid base as an excellent tool for information hiding. An analogue image can be described as a continuous function over a two-dimensional surface. The value of this function at a specific coordinate on the lattice specifies the luminance or brightness of the image at that location. A digital image version of this analogue image contains sampled values of the function at discrete locations or pixels. These values are said to be the representation of the image in the spatial domain or often referred to as the pixel domain. Spatial embedding inserts message into image pixels. The oldest and the most common used method in this category is the insertion of the watermark into the least significant bits (LSB) of pixel data [2][5][6]. The embedding process of the LSB technique can be illustrated as follows: Consider that the system is required to hide a watermark number 178 in a 2x2 gray-scale (8-bit) image. Let's assume that the image pixels are 234, 222, 190 and 34. In an 8-bit binary format the number 178 is represented as 10110010. Since there are 4 pixels that can be used to store this data we can easily decide to embed pairs of bits of the watermark to the last 2 insignificant bits of the pixels. The process therefore modifies the original bits from 11101010, 11011110, 10111110 and 00100010 to 11101010, 11011111, 10111100 and 00100010 respectively. In decimal representation the watermarked image has pixel values of 234, 223, 188 and 34. Since the modification of pixel values occurs in the LSB of the data, the effect to the cover image is often visually indifferent. This effect however becomes more apparent as more bits are used to hide the watermark. One of the major limitations in spatial domain is the Capacity of an image to hold the watermark. In the case of LSB technique, this capacity can be increased by using more bits for the watermark embedding at a cost of higher detection rate.

3.2 Frequency Domain

a. Discrete Cosine Transform (DCT): The sequence of data points in the spatial domain are converted to the sum of sine and cosine waveforms with different amplitudes in the frequency domain. Unlike Discrete Fourier Transform, this transform has only real numbers when a cosine function is used. There are eight different variants of DCT with slight modifications between them. Discrete Cosine Transform is related to DFT in a sense that it transforms a time domain signal into its frequency components. The DCT however only uses the real parts of

the DFT coefficients. In terms of property, the DCT has a strong "energy compaction" property and most of the signal information tends to be concentrated in a few low-frequency components of the DCT. The JPEG compression technique utilizes this property to separate and remove insignificant high frequency components in images. Srayazdi proposed a blind gray-level watermarking scheme by dividing the cover image into 4x4 non-overlapping blocks. The technique first estimates the first five DCT coefficients of each block in a zigzag order. It then embeds a gray-level value of the watermark data by replacing each low frequency DCT value in the central block with its estimated modified values. In , the author created a new robust hybrid non-blind watermarking scheme based on discrete cosine transform (DCT) and Singular Value Decomposition (SVD). The Discrete cosine transform (DCT) is most popular due to several reasons. One of the reason is that most of the compression techniques developed in the DCT domain (JPEG, MPEG, MPEG1, and MPEG2) & therefore image processing is more familiar with it. DCT is one of the most common linear transformations in digital signal process technology. Two-dimensional discrete cosine transform (2D discrete cosine transform is defined as follows

$$f(jk) = a(j)a(k)\sum_{m=0}^{N-1}\sum_{n=0}^{N-1} f(nm)\cos\left[\frac{(2m+1)j\pi}{2N}\cos\left[\frac{(2N+1)k\pi}{2N}\right.\right.$$

Inverse transformation 2D discrete cosine transform is defined as follows

$$f(mn) = \sum_{m=0}^{N-1}\sum_{n=0}^{N-1} a(j)\,a(k)\,f(jk)\cos\left[\frac{(2m+1)j\pi}{2N}\cos\left[\frac{(2N+1)k\pi}{2N}\right.\right.$$

b. Discrete Wavelet Transform (DWT): In this transform the signal is decomposed into a set of basic wavelets followed by the altering of lower frequencies at various resolutions. Transform domain embeds a message by modifying the transform coefficients of the cover message as opposed to the pixel values. Ideally, transform domain has the effect in the spatial domain of apportioning the hidden information through different order bits in a manner that is robust. There are a number of transforms that can be applied to digital images, but there are notably three most commonly used in image watermarking. They are Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT).

$$H_i = \sum_{m=0}^{k-1} X_{2i-m} \cdot s_{m(Z)}$$

$$L_i = \sum_{m=0}^{k-1} X_{2i-m} \cdot t_{m(Z)}$$

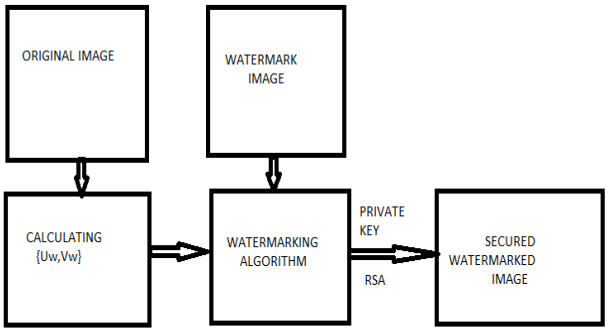
Where $s_{m(Z)}$ $t_{m(Z)}$=wavelet filters
i =0 (N|2)-1
k=length of filter

Watermarking in the wavelet transform domain is generally a problem of embedding watermark in the sub bands of the cover image. There are four sub bands created at the end of each level of image wavelet transformation: they are Low-Low pass sub band (LL), High-Low (horizontal) sub band (HL), Low-High (vertical) sub band (LH) and High-High (diagonal) pass sub band (HH). Subsequent level of wavelet transformation is applied to the LL sub band of the previous one. [11the input image decompose into 4 levels by DWT, so we get approximation sub bands with low frequency component and 12 detail sub bands with high frequency component morphological dilation capture the coefficients that near the edge for forming another group. In the end, the watermark energy distribute among these groups with a suitable length. For this project, a form of spatial domain watermarking technique will be used.

4. LITERATURE SURVEY OF FRAGILE WATERMARKING TECHNIQUES IN TRANSFORM DOMAIN

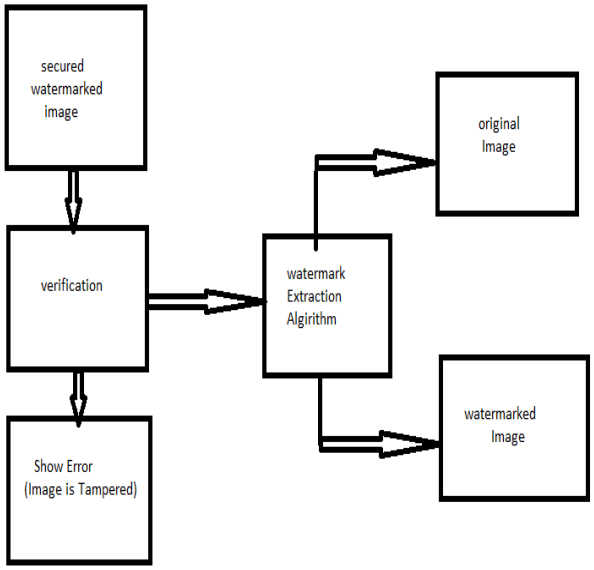
Frequency domain techniques have proved to be more effective than spatial domain techniques in achieving high robustness against attacks and can embed more bits of watermark. Commonly used frequency domain transforms are Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Discrete Fourier transform (DFT). DWT has been given special attention in digital image watermarking due to its excellent spatial localization and multi-resolution characteristics, which are similar to the theoretical models of the human visual system. Transform domain techniques have been applied for copyright protection and image authentication. A brief description of some techniques for image authentication is covered below. In 2008, Wang H. et al., [9] proposed a chaotic watermarking scheme for authentication of JPEG images. The quantized DCT coefficients after entropy decoding are mapped to the initial values of the chaotic system, and then the generated watermark information by chaotic iteration is embedded into JPEG compressed domain. Requantization operation does not invalidate tamper detection due to direct modification of DCT coefficient after quantization. Extraction is also performed in the compression domain. Extraction is fast and complexity of method is claimed to be low. In 2012, Kannammal et. al. [14] proposed a digital watermarking framework in which the Electrocardiograph (ECG) and Patients demographic text ID act as double watermarks. By this method the medical information of the patient is protected and mismatching of diagnostic information is prevented.

5. BLOCK DIAGRAM



Fig(a): Embedding the watermark image

Fig(a): Embedding the watermark image



Fig(b):Extraction of Watermarked Image

Fig(b): Extraction of watermarked image

There are three main stages in the watermarking process:

1. generation and embedding
2. attacks
3. retrieval/detection

Generation of watermarks is an important stage of the process. Watermarks contain information that must be unique otherwise the owner cannot be uniquely identified. In embedding, an algorithm accepts the host and the data to be embedded and produces a watermarked signal. Various algorithms have been developed so far. The watermarked signal is then transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an attack. There are many possible attacks. Detection is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal is not modified during transmission, then the watermark is still present and it can be extracted. If the signal is copied, then the information is also carried in the copy. The embedding takes place by manipulating the contents of the digital data, which means the information is not embedded in the frame around the data, it is carried with the signal itself.

6. WATERMARKING ALGORITHM

The mathematical details of the algorithm used in obtaining the public and private keys are available at the RSA Web site. Briefly, the algorithm involves multiplying two large prime numbers (a prime number is a number divisible only by that number and 1) and through additional operations deriving a set of two numbers that constitutes the public key and another set that is the private key. Once the keys have been developed, the original prime numbers are no longer important and can be discarded. Both the public and the private keys are needed for encryption /decryption but only the owner of a private key ever needs to know it. Using the RSA system, the private key never needs to be sent across the Internet. The private key is used to decrypt text that has been encrypted with the public key. Thus, if I send you a message, I can find out your public key (but not your private key) from a central administrator and encrypt a message to you using your public key. When you receive it, you decrypt it with your private key. In addition to encrypting messages (which ensures privacy), you can authenticate yourself to me (so I know that it is really you who sent the message) by using your private key to encrypt digital certificate**.** When I receive it, I can use your public key to decrypt it. The above mentioned program is written in MATLAB and is executed. The following points explain the program code:

1. It asks the user to input the Host image and the Watermark image.
2. It reads the images input by the user and displays them. It then doubles the images for the subsequent operations
3. It then assigns the number of bits of host image to be replaced by the watermark image.
4. Each pixel is an 8-bit byte; hence the watermark image is shifted to 8-(number of bits assigned) places to the right.

7. FEATURES OF THE PROJECT

Every watermarking technique is designed by keeping a particular application in mind. The features and their relative importance that watermarking technique should possess are also application dependent. Giving paramount attention to this, we now present desirable features of fragile marking systems

1. Tamper detection
2. Perceptual Transparency
3. Detection should not require the original image

4. Detector should be able to locate and characterize alterations made to a marked image
5. The watermarks generated by different marking keys should be "orthogonal" during watermark detection
6. The marking key spaces should be large
7. The marking key should be difficult to deduce from the detection side information

8. SIMULATION RESULTS

To illustrate the effectiveness on the tamper discrimination property of the proposed method, several experiments were carried out using the test image of Fig. 1 (a). The types of tamper are the manipulation occurred on: (I)Both the image content and the watermark: a fake plate number "R237 JAD" is pasted on the watermarked image of Fig. 1 (a). This tampered image is shown in Fig.4 (a). (2)The image content: we replace the 7 most significant bits (MSBs) of each pixel in Fig. 1 (a) with that in Fig.4 (a). The resulting image is depicted in Fig.4 (b). (3)The watermark: we replace the LSB of each pixel in Fig.1 (a) with that in Fig.4 (a). That is, we alter the watermark of the test image. The tampered image is shown in Fig.4 (c). According to watermarks embedded the LSB of tested image, the reconstructed LSQMs of these images are shown in Figs.4 (d), (e), and (f), respectively. We observe that the proposed watermarking algorithm has the capability of retrieving the original plate number from the altered image in which the plate number is modified. Figs.5 (a), (b), and (c) are the difference matrixes of three tamper by the verification algorithm respectively. Tamper localization and tamper discrimination can be achieved by viewing the difference images. As can be seen from Fig.5 (a), altered plate is located. The isolated dots spread all over the image indicate that the embedded watermark was changed. On the other hand, as shown in Fig.5 (c), only spread isolated dots appears. This implies that the manipulation on the image is only restricted to the watermark. Thus the image content is genuine. When a logo is used as the watermark, Figs.5 (d), (e), and (f) are shown the authentication results of three tampers using Wong's algorithm [3]. It can locate where the alteration of the image is. But we cannot tell what kind of manipulations being made on the marked image; and they might be declared fake, even though Fig. 4(c) contains genuine digital contents.

Fig. 4. Image authentication results by the proposed watermarking algorithm (a) ,(b) and (c) are the tampered images of three corresponding tampers, respectively; (d),(e) and (f) are the reconstructed LSQMs of three corresponding tampers, respectively.

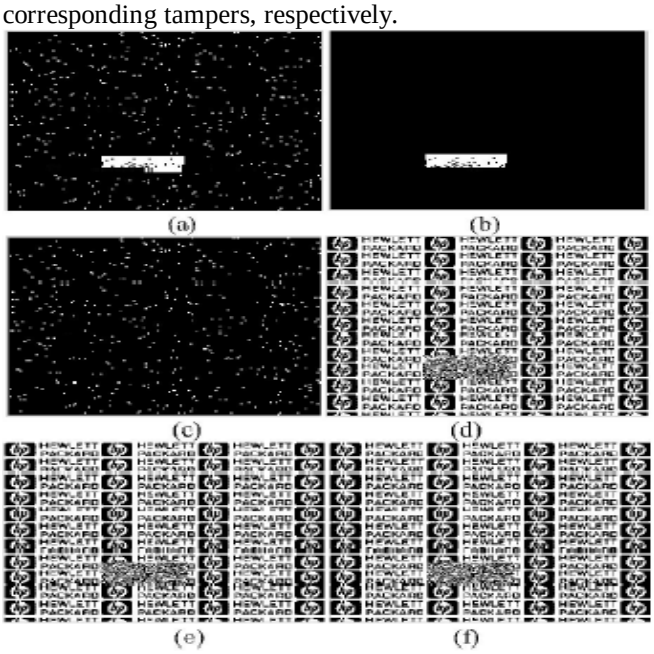


Fig. 5. Authentication results in comparison of tamper localization and discrimination (a), (b) and (c) are authentication results of three tamper by the proposed algorithm; (d), (e) and (f) are the results of three tamper by Wong's algorithm [3]

9. POSSIBLE ATTACKS ON FRAGILE WATERMARKS

Fragile watermarks are embedded in the cover media to detect any occurrence of tampering in it. If the alterations are so performed on the watermarked image that they do not disturbed the embedded watermark, then the altered

image can still be authenticated defeating the purpose of watermark embedding. Many block wise independent techniques are to be vulnerable to counterfeiting attacks [8]. Some counterfeiting attacks common to fragile watermarks are briefly defined in this section: (a) Cut and paste attack: In cut-and-paste attack, the attacker modifies the content of a watermarked image by cutting regions from the same or another watermarked image and pasting them together to form a new image. (b) Birthday attack/collage attack: The attacker searches for collisions i.e. pairs of blocks that hash to the same value, thus having the same signature. A hash function that produces a bit string of length l, the probability of finding at least two blocks that hash to the same output is greater than 0.5 whenever roughly 2l/2 watermarked blocks are available. The idea of the attack is to forge a new watermarked image (a collage) from a number of authenticated images watermarked with the same key and watermark/logo by combining portions of various authenticated images while maintaining their relative positions in the forged version. In general, the only protection against birthday attacks is to increase the hash size. The attack is also termed as collage or VQ attack. In vector quantization attack, a VQ codebook generated from a set of watermarked images. Since each block is authenticated by itself, the counterfeit image appears authentic to the watermarking scheme. Other sophisticated attacks have also been designed like transplantation attacks, which require the block wise dependency to be nondeterministic.

10. CONCLUSION

In this paper, we propose a cryptography based technology that has been publicly applied in information security to assist the examination and analysis of digital image data. The technology provides a unique cipher for every single processed image. We can use the unique cipher (check any change of the cipher) to confirm if the image is modified easily. With the proposed technology, we can strengthen image authentication effectively.

REFERENCES

[1]. M.M. Yeung and F. Mintzer, "An invisible watermarking technique for image verification," Proc.

[2]. P. Wong, "A public key watermark for image Verification and authentication," Proc. IEEE Int. Conf Image Processing, Chicago, IL, 1998, pp. 425 - 429.

[3] . P. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification," IEEE Trans. Image Processing, vol. 10, pp. 1593-1601, 2001

[4] M. Celik, G. Sharma, E. Saber, and A.M. Tekalp, Hierarchical watermarking for secure image authentication with localization," IEEE Trans. Image Processing, vol. 11, no. 6, pp. 585-595,

[5] E. Izquierdo and V. Guerra, "An ill-posed operator for secure image authentication," IEEE Trans. Circuits and Systems for Video Technology, vol. 13, no. 8, pp. 842- 852, August 2003.

[6] H. Holliman and N. Memon, "Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes," IEEE Trans. Image Processing, vol. 9, no. 3, pp. 432-441, March 2000.

[7] J. Fridrich, "Security of fragile authentication watermarks with localization," Proc. SPIE, vol. 4675, Security and Watermarking of Multimedia Contents, San Jose, CA, Jan., 2002, pp. 691-700