International Journal of scientific research and management (IJSRM)
\||Volume||3||Issue||4||Pages|| 2571-2581||2015||
Website: www.ijsrm.in ISSN (e): 2321-3418

Generic Lossless Visible Watermarking

Ms. Mrunali U. Bhaisare[1], Prof. Vivek R. Raut[2]

[1]PG Student, Dept. of Electronics and Telecommunication, PRMIT&R Badnera, Amravati,

Saint Gadge Baba Amravati University, Maharashtra, India

mrunalibhahisare15@gmail.com

[2]Dean Academics at PRMIT&R Badnera, Amravati,

Saint Gadge Baba Amravati University, Maharashtra, India

rautvivek@rediffmail.com

Abstract: For generic visible watermarking with a capability of lossless image recovery, a novel method is proposed. This method is based on the deterministic one-to-one compound mappings of image pixel values for covering a variety of visible watermarks of arbitrary sizes on the host images. The compound mappings are proved to be reversible, that means it allows lossless recovery of original images from watermarked images, so that recovered image and the host image should be the same. The mappings may be adjusted to yield pixel values close to those of desired visible watermarks. Including opaque monochrome and translucent full color ones, different types of visible watermarks are embedded as applications of the proposed generic approach. To produce more distinctive visible watermarks in the watermarked image, a two-fold monotonically increasing compound mapping is created and proved. Security protection measures by parameter and mapping randomizations and also by using the HASH algorithm have also been proposed to prevent attackers from illegitimate image recoveries. Experimental results representing the convenience of the proposed approach are also included.

Keywords: Lossless reversible visible watermarking, mapping randomization, one-to-one compound mapping, parameter randomization, translucent watermark, two-fold monotonically increasing..

1. Introduction

The introduction of the Internet has resulted in many new opportunities for the making and delivery of content in digital form. Applications of digital data include electronic advertising, real time video and audio delivery, digital repositories and libraries, and Web publishing. An important issue that arises in these applications is the protection of the rights of the digital data of all participants. It has been recognized that current copyright laws are inadequate for dealing with digital data. This has headed to an interest towards developing new copy prevention and protection mechanisms. One such effort that has been attracting increasing interest is based on digital watermarking techniques. Digital watermarking is the process of embedding information into digital multimedia content such that the information can later be extracted or detected for a variety of purposes including copy prevention and control. Digital watermarking has become an active and important area of research, and development and commercialization of watermarking techniques is being deemed essential to help address some of the challenges faced by the rapid proliferation of digital content.

Digital watermarking methods for images are usually categorized into two types: invisible and visible. The first type aims to embed copyright information imperceptibly into host media such that in cases of copyright infringements, the hidden information can be retrieved to identify the ownership of the protected host. It is important for the watermarked image to be resistant to common image operations to ensure that the hidden information is still retrievable after such alterations. Methods of the second type, on the other hand, yield visible watermarks which are generally clearly visible after common image operations are applied. In addition, visible watermarks convey ownership information

directly on the media and can deter attempts of copyright violations [22]. Embedding of watermarks, either visible or invisible, degrade the quality of the host media in general. Desired Characteristics of Visible Watermarks Some of the desired characteristics of visible watermarks could be as follows:

1. Visible in both color and monochrome images
2. Visible only on careful examination of the image
3. Should not significantly obscure the image details beneath it
1. Should be difficult to remove automatically- should be robust
2. The insertion process should be automated for all kinds of images

A group of techniques, named reversible watermarking [8]-[19], allow legitimate users to remove the embedded watermark and restore the original content as needed. However, not all reversible watermarking techniques guarantee lossless image recovery, which means that the recovered image is identical to the original, pixel by pixel. Lossless recovery is important in many applications where serious concerns about image quality arise. Some examples include forensics, medical image analysis, historical art imaging, or military applications. As to lossless visible watermarking, the most common approach is to embed a monochrome watermark using deterministic and reversible mappings of pixel values or DCT coefficients in the watermark region [6],[9],[19]. Another approach is to rotate consecutive watermark pixels to embed a visible watermark [19].

One advantage of these approaches is that watermarks of arbitrary sizes can be embedded into any host image. However, only binary visible watermarks can be embedded using these approaches, which is too restrictive since most company logos are colorful. In this project, a new method for lossless visible watermarking is used by using appropriate compound mappings that allow mapped values to be controllable. The mappings are proved to be reversible for lossless recovery of the original image. The approach is generic, leading to the possibility of embedding different types of visible watermarks into cover images. Two applications of this method are demonstrated, where opaque monochrome watermarks and non-uniformly translucent full-color ones are respectively embedded into color images.

More specific compound mappings are also created and proved to be able to yield visually more distinctive visible watermarks in the watermarked image. To the best knowledge of the authors, this is the first method ever proposed for embedding removable translucent full color watermarks which provide better advertising effects than traditional monochrome ones.

3. Problem Definition

Among all the requirements of watermarking system, imperceptibility is a basic requirement and independent of the application purpose. Other requirements also need to be taken into consideration when designing watermarking techniques.

* Imperceptibility:

One of the most important requirements is the perceptual transparency of the watermark which can also be called as fidelity which refers to the similarity of the un-watermarked and watermarked works. From this perspective, the watermark system exploits the imperfect of human eyes. However, for some watermarking system, the watermarks are made to be visible on purpose. Still, invisible watermarking system is the majority.

* Robustness:

For all the robust watermarking applications, the ultimate watermarking method is supposed to survive any kind of alterations or intentional removal introduced by standard or malicious processing and attacks. However robust watermark is distinguished from secure watermark. Robust watermarks are designed to resist normal processing. On the other hand, secure watermarks are designed to resist any attempt by an adversary to thwart their intended purpose. However robustness is a necessary property if a watermark is to be secure.

* Blind or Informed Detection:

In some applications, the original, un-watermarked work is available during detection. In other applications, detection must be performed without access to the original work. The former watermark system is referred to as informed detection and the latter is called blind detection. In the watermarking literature, systems that use informed detection are often called private watermarking systems, whereas those that use blind detection are called public watermarking systems. For the fragile watermarking, definitely we need use the public watermarking. However, this kind watermarking also increases the possibility of malicious access.

*Watermark Keys:

If secrecy is a requirement, a secret key has to be used for the embedding and detection process. There are three types of keys using in watermark systems: private-key, detection-key and public-key. A private-key is available only to the author and can be thought of as a flair or signature to the product. The detection-key is the method that is recognized in the court of law. The public-key is the one that can be extracted by the public. In general, a given watermarking system should have a certain property to be suitable for a given application. Besides the properties or requirements we have mentioned above, digital watermarking also has other properties such as payload, which refers to the capacity, or the amount of data that can be inserted into the cover data.

4. Proposed Approach

1. Reversible one to one Compound mapping

The title of the paper is centered 17.8 mm (0.67") below the top of the page in 24 point font. Right below the title (separated by single line spacing) are the names of the authors. The font size for the authors is 11pt. Author affiliations shall be in 9 pt. First, we propose a generic one-to-one compound mapping f for converting a set of numerical values$P = \{p_1, p_2, \dots \dots p_M\}$to another set $Q = \{q_1, q_2, \dots \dots q_M\}$, such that the respective mapping from p_i to q_i for all i =1, 2……M is reversible. Here, for the copyright protection applications investigated in this study, all the values p_i and q_i, are image pixel values(grayscale or color values). The compound mapping f is governed by a one-to-one function F_x with one parameter x= a or b in the following way:

$$q = f(p) = F_b^{-1}\big(F_a(p)\big) \qquad (1)$$

Where,

$F_x^{-1}$is the inverse of F_x

Which by the one-to-one property ,leads to the fact that if $F_a(p) = p'$,then $F_a^{-1}(p') = p$, then for all values of a and p. On the other hand, $F_a(p)$ and $F_b(p)$ generally are set to be unequal if a ≠ b.

The compound mapping described by (1) is indeed reversible, that is, p can be derived exactly from using the following formula:

$$p = f^{-1}(q) = F_a^{-1}\big(F_b(q)\big) \qquad (2)$$

as proved below.

1. Lemma 1 (Reversibility of Compound Mapping):

If $q = F_b^{-1}\big(F_a(p)\big)$ for any one-to-one function F_x with a parameter x, then $p = F_a^{-1}\big(F_b(q)\big)$ for any values of a, b, p and q.

Proof: Substituting (1) into $F_a^{-1}\big(F_b(q)\big)$, we get

By regarding $F_a(p)$as a value c, the right-hand side becomes, $F_a^{-1}\left(F_b\left(F_b^{-1}(c)\right)\right)$, which, after$F_b$ andF_b^{-1} are cancelled out,becomes $F_a^{-1}(c)$. But $F_a^{-1}(c)$=$F_a^{-1}(F_a(p))$, which is just p after F_a and F_a^{-1} are cancelled out. That is, we have proved $p = F_a^{-1}\big(F_b(q)\big)$.

As an example,

If $F_x(p) = xp + d$, then $F_x^{-1}(p') = (p' - d)/x$.

Thus

$$q = F_b^{-1}\big(F_a(p)\big) = F_b^{-1}(ap + d)$$

$$= [(ap + d - d)/b] = ap/b$$

and so, we have

$$F_a^{-1}(F_b(q)) = F_a^{-1}\left(b\left(\frac{ap}{b}\right) + d\right) = F_b^{-1}(ap + d)$$

$$= [((ap + d) - d)/a] = (ap/a) = p$$

as expected by Lemma 1.

2. Lossless Visible Watermarking Scheme

Based on Lemma 1, we will now derive the proposed generic lossless visible watermarking scheme in the form of a class of one-to-one compound mappings, which can be used to embed a variety of visible watermarks into images. The embedding is reversible, that is, the watermark can be removed to recover the original image losslessly. For this aim, a preliminary lemma is first described as follows.

1. Lemma 2 (Preference of Compound-Mapped Value q):

It is possible to use the compound mapping $q = F_b^{-1}(F_a(p))$ to convert a numerical value p to another value close to a preferred value l.

Proof: Let$F_x(p) = p - x$ where x is the parameter for F. Then $F_x^{-1}(p') = p' + x$. Also, let $a = p - €$ and $b = l$ where € is a small value. Then, the compound mapping $F_b^{-1}(F_a(p))$ of p yields q as

$$q = F_b^{-1}(F_a(p)) = F_b^{-1}(p - a) = F_b^{-1}(€)$$

$$= € + b = € + l$$

which means that the value q is close to the preferred value l .

The above lemma relies on two assumptions. The first is that a is close to p, or equivalently, that $a = p - €$. The reasonwhy we derive the above lemma for $a = p - €$ instead of for a= p , is that in the reverse mapping we want to recoverp fromq without knowing p, which is a requirement in the applications of reversible visible watermarking investigated in this study. Although the value of p cannot be known in advance for such applications, it can usually be estimated, and we will describe some techniques for such estimations in the subsequent sections.

The second assumption is that $F_x(p)$yields a small value ifx and p are close. Though the basic difference function $F_x(p) = p - x$ used in the above proof satisfies this requirement for most cases, there is a possible problem where the mapped value may exceed the range of valid pixel values for some values of a, band p.

For example,

When a=255, b=255, p=253,

We have,

q=255-253+255=257>255

It is possible to use the standard modulo technique (i.e., taking q = $257_{\mathrm{mod}_{253}} = 1$) to solve this issue; however, such a technique will make q far from the desired target value of b, which is 255. Nevertheless, we will show in chapter 7 that using such a standard modulo function, $F_a(p) = (p - x)_{\mathrm{mod}\,256}$ can still yield reasonable experimental results. Furthermore, we show in chapter 7 in theorem 1 a more sophisticated one-to-one function that is free from such a wrap-around problem.

By satisfying the above two requirements, the compound mapping yields a value q that is close to the desired value l. We now prove a theorem about the desired lossless reversible visible watermarking in the following.

Theorem 1 (Lossless Reversible Visible Watermarking):

There exist one-to-one compound mappings for use to embed into a given image I a visible watermark Q whose pixel values are close to those of a given watermark L, such that the original image I can be recovered from Q losslessly .

Proof: This is a consequence of Lemmas 1 and 2 after regarding the individual pixel values in I, L, and Q respectively as those of p, l and q, mentioned in Lemma 2. And it is clear by Lemma 1 that the value p can be recovered losslessly from the mapped value q which is derived in Lemma 2.

The above discussions are valid for embedding a watermarking a grayscale image. If color images are used

both as the cover image and the watermark, we can apply the mappings to each of the color channels to get multiple independent results. The resulting visible watermark is the composite result of the color channels.

Based on Theorem 1, the proposed generic lossless reversible visible watermarking scheme with a given image I and a watermark L as input is described as an algorithm as follows.

Related Algorithm:

1. Algorithm 1: Generic Visible Watermark Embedding

Input: an image **I** and a watermark **L**.

Output: watermarked image **W**.

Steps:

1) P of pixels from I where L is to be embedded, and call P

a watermarking area.

2) Denote the set of pixels corresponding to P in W by Q.

3) For each pixel X with value p in P, denote the corresponding pixel in Q as Z and the value of the corresponding pixel Y in L as l, and conduct the following steps.

a) Apply an estimation technique to derive a to be a value close to p, using the values of the neighboring pixels of X (excluding X itself).

b) Set to be the value l.

c) Map to a new value$\mathrm{q} = \mathrm{F}_{\mathrm{b}}^{-1}\big(\mathrm{F}_{\mathrm{a}}(\mathrm{p})\big)$.

d) Set the value of Z to be q.

4) Set the value of each remaining pixel in W, which is outside the region P, to be equal to that of the corresponding pixel in I.

Fig. Illustration of mapping the center pixel of a 3*3 image using Algorithm 1.Only the mapping of the center pixel is shown for clarity; the east & south pixels are depicted as TBD(to be determined) in W.

We do not use the information of the original image pixel value of X itself for computing the parameters a and b for X. This ensures that identical parameter values can be calculated by the receiver of a watermarked image for the purpose of lossless image recovery.

As an example, the process performed by Step 3 of the above algorithm for a pixel is illustrated by Fig.3.1, where the north and west pixels are used to estimate the color of the center pixel. Note that the east and south pixels are not used because these pixels are covered by the watermark and unknown to the receiver. It is important to allow as many neighbors of a pixel as possible to be known by the receiver to ensure that a good estimate can be calculated for that pixel. We will describe techniques for processing pixels, which can ensure that sufficiently many neighbor colors are known by a receiver for each pixel in the watermarking area.

The corresponding watermark removal process for a watermarked image W generated by Algorithm 1 is described as an algorithm as follows.

2. Algorithm 2: Generic Watermark Removal for Lossless Image Recovery

Input: a watermarked image **W** and a watermark **L**.

Output: the original image **R** recovered from **W**.

Steps:

1. Select the same watermarking area Q in W as that selected in

Algorithm 1.

2. Set the value of each pixel in R , which is outside the region Q,

to be equal to that of the corresponding pixel in W.

3. For each pixel Z with value q in Q, denote the corresponding pixel in the recovered image R as X and the value of the corresponding

Pixel Y in L as l, and conduct the following steps.

a) Obtain the same value as that derived in Step 3a of algorithm 1 by applying the same estimation technique used there.

b) Set b to be the value l.

c) Restore p from q by setting$p = F_a^{-1}(F_b(q))$.

d) Set the value of X to be p.

4. Algorithm 3: Watermark Embedding of a Translucent Color Watermark

Input: an image **I** and a translucent watermark **L**.

Output: a watermarked image **W**.

Steps:

1) Select the watermarking area P in I to be the set of pixels corresponding spatially to those in L which are nontransparent (with alpha values larger than zero).

2) Denote the set of pixels corresponding to P in W as Q.

3) For each pixel X with value p in P, denote the corresponding pixel

In Q as Z and the value of the corresponding pixel Y in L as l , and

conduct the following steps.

1. Set the parameter a to be a neighbor-based color estimate value

that is close top by using the colors of the neighboring pixels of

X that have already been processed

2. Perform alpha blending with l over a to get the parameter b according to the formula b=l*α +a*(255-α)

Where α is the opacity of Y.

c) Map to a new value$q = F_b^{-1}(F_a(p))$.

d) Set the value Z of to be q.

4) Set the value of each remaining pixel in W, which is outside the

Region P, to be equal to that of the corresponding pixel in I .

For Step 3a above, there are several ways to determine the color estimate of a pixel using the colors of its neighbors that have already been processed, such as simply averaging the colors of the processed 4 neighbors of the pixel, or averaging those of the processed 8-neighbors with more weights on the horizontal and vertical members. We may also use more sophisticated techniques such as edge-directed prediction for this purpose, as long as we use only processed pixels.

The reason for using only processed pixels is that these pixels are the ones that a receiver can reliably recover during watermark removal. This is to ensure that the same color estimates can be computed for lossless recovery. Specifically, the value q of the first processed pixel is computed from the neighboring pixels outside the region P. Since the values of these pixels outside Pare unchanged, a receiver can, therefore, reliably recover the first pixel using a reverse mapping using q and the values of neighboring pixels outside P. Each of the other unprocessed pixels is handled by using the processed pixels in a similar way.

To ensure that there always exists processed neighbors for accurate color estimates, we limit the pixels to be selected and processed next to be those with at least two already-processed neighbors in a four-pixel

neighborhood. A consequence of this is that pixels around the outer edges of the watermark region are processed before those in the center. This can be clearly seen in Fig. , where some of the intermediate outputs yielded during watermark embedding and removing are shown [the most obvious outer edges are seen in Fig. 6.2(a)].

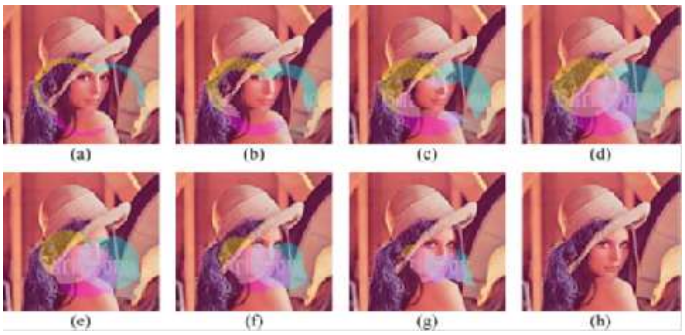

Fig. Illustration of pixel processing order in watermark embedding and removal. (a)–(d) Intermediate results of image watermarking when 25%, 50%, 75%, and100% of the watermark pixels have been processed, respectively. (e)–(h) Intermediate results of image recovery when 25%, 50%, 75%, and 100% of the watermark pixels have been recovered, respectively.

1. Two Fold Monotonically Increasing Property

We mapped a pixel value to a preferred value by using a simple one-to-one function $F_x(p) = (p - x)_{\mathrm{mod}\ 256}$. A problem of this mapping is that for certain values of a, b and p, the mapped value will wrap around and deviate from the intended value. To solve this problem, we propose an alternative one-to-one function F_x such that the compound mapping $q = F_b^{-1}(F_a(p))$ does not exhibit the wrap-around phenomenon. Specifically, the mapping always yields a value close to b

if a and p are close to each other for all values of a, b and p. We will call this a two-fold monotonically increasing property, and will prove by a theorem that such a property holds if the one-to-one function F_x has a one-fold monotonically increasing property. The definitions of both of these properties and the detail of the theorem are described in the following.

Definition (One-Fold Monotonically Increasing One-to-One Function):

A one-to-one function F_a is one-fold monotonically increasing if for all values of a, p_1 and $p_2, F_a(p_1) < F_a(p_2)$implies $|a - p_1| \le |a - p_2|$

Lemma 3 (Inverse Monotonicity):

The inverse of a one-fold monotonically increasing function Fx exhibits the following characteristic of inverse monotonicity:

for all values of b,p_1' andp_2',$p_1' < p_2'$implies

$$|b - F_b^{-1}(p_1')| < |b - F_b^{-1}(p_2')|$$

Proof:

Let $p_1' = F_b(p_1)$ and $p_2' = F_b(p_2)$ for some b,$p_1$andp_2.Then

$$|b - p_1| \le |b - p_2|$$

by Definition 1. Also, we have$F_b^{-1}(p_1')$=$F_b^{-1}(F_b(p_1)) = p_1$, and $F_b^{-1}(p_2') = F_b^{-1}(F_b(p_2)) = p_2$, similarly, Substituting p_1 and p_2 into the above inequality, we get$|b - F_b^{-1}(p_1')| \le |b - F_b^{-1}(p_2')|$ .This completes the proof.

7.1.2 Definition (Two-Fold Monotonically Increasing):

The compound mapping $q = F_b^{-1}(F_a(p))$ is two-fold monotonically increasing if for all values of a, b,p_1 and p_2, $|a - p_1| < |a - p_2|$ (i.e., if a is closer top_1 thanp_2) implies$|b - q_1| \le |b - q_2|$ (i.e., b is at least as close to q_1 as q_2), where $q_1 = F_b^{-1}(F_a(p_1))$ and $q_2 = F_b^{-1}(F_a(p_2))$.

Theorem (Two-Fold Monotonically Increasing):

If F_x is a one-fold monotonically increasing one-to-one function with a parameter x, then the compound mapping $q = F_b^{-1}(F_a(p))$ is two-fold monotonically increasing. The proof of the above theorem is included in the Appendix.

We now show the existence of a one-fold monotonically increasing function and how it works for any pixel value and in the range of 0 to 255, by way of an algorithm below.

Related Algorithms

Algorithm 4: One-to-One Mapping Exhibiting One-Fold Monotonically Increasing Property

Input: a parameter a and an input value p, each in the range of 0 to 255.

Output: a mapped output p' in the range from 0 to 255.

Steps:

1) Initialize p'to be zero.

2) Create a set S with initial elements being the 256 values of 0 through 255.

3) Find a value r in such that | a- r | is the minimum, preferring a smaller r in case of ties.

4) If r is not equal top, then remove r from S , increment p' by one, and go to Step 3; otherwise, take the final p' as the output.

As an example, if we want to determine the function value $F_a(p)$ for a=3 and p=1 by the above algorithm, then we will find r=3 in Step 3 of the above algorithm. But r=3≠ $1 = p$ so 3 is removed from S with p' being incremented from 0 to 1. The subsequent iterations will compute r to be 2, 4, and finally 1 which is equal to p, with the final value of being taken to be 3 as the output.

The inverse of the one-to-one function described by Algorithm4 is described below.

Algorithm 5: Inverse of the Mapping Function Described by Algorithm 1

Input: a parameter b and an input value p', each in the range of 0 to 255.

Output: an output value p that is in the range from 0 to 255.

Steps:

Create a set S with the initial elements being the 256 values of 0

through 255.

Find a value p in such that |b-p| is the minimum, preferring a smaller in p case of ties.

If p' is larger than zero, then remove p from S, decrement p' by one, and go to Step 2; otherwise, take the final p as the output.

As an example, if we want to compute$F_b^{-1}((p'))$ forb=3 and p'=3by the above algorithm, then we will find in Step 2 the sequence of 3, 2, 4, and 1 for the values of p , with decreasing from 3, 2, 1, and then 0. The output is hence p=1.

Note that in practice, we can precompute all 256*256 possible one-to-one mappings in both Algorithms 4 and 5 beforehand, so that the mapping Fx and its inverse F_x^{-1} can be implemented by efficient lookup-table operations of constant-time complexity. As proved by Theorem 2 and two extra lemmas (Lemmas 4 and 5) included in the Appendix, we can use the mapping and its inverse described in Algorithms 1 and 2, respectively, to map the pixel values of an image to the desired values of a watermarked image, such that the watermark is visually clear if a is close top. It is guaranteed that the original image can be recovered losslessly from the watermarked image, as proved by Theorem 1

3. Security Consideration

Although we want legitimate users to be able to recover the original image from a watermarked one, we do not want an attacker to be able to do the same. Herein, we propose some security protection measures against illicit recoveries of original images.

We want legitimate users to be able to recover the original image from a watermarked one, we do not want an attacker to be able to do the same. Herein, we propose some security protection measures against illicit recoveries of original images.

4. Hash Algorithm

The hash functions are one-way functions, which return a fixed length result H (M) when they are applied on an arbitrary length message M. The one-way hash functions respect the following properties [24]:

1. If the message M is given, it is easy to compute H(M).

2. It is hard to find the message M if H(M) is given.

3. If a message M is given, it is hard to find another message M', such that H(M) = H(M');

4. It is hard to find two random messages M and M', such that H(M) =

H(M');

5. It is easy to implement the hash function in hardware and in software

There are several examples of one-way hashing algorithms some of them are MD4, MD5 and SHA but we will describe briefly only SHA in this project. MD4 is a hashing algorithm designed by Ron Rivest, which produces a 128-bit message digest of the input message. Its simplicity, compactness and speed are good but, several methods that cryptanalyze certain parts of this algorithm were proposed. In order to counterattack the above mentioned cryptanalytical approaches, a new algorithm was designed. Its name is MD5 and improves MD4 by increasing the number of rounds contained in the main loop from 3 to 4. MD5 produces also a hash of 128 bits.

The National Security Agency (NSA) proposed another algorithm in which case the message digest is 160 bits long. This algorithm is called SHA (Secure Hash Algorithm) and his security seems to be better than in the case of MD5 because, as it can be seen above, its hash length is larger by 32 bits. The implementations that use SHA run slower than the ones based on MD5 because the number of operations to be done is bigger.

We used in our pseudo-noise generating method the hash functions because, in our application, the watermark must depend on the original image in order to improve its security. No matter if MD4, MD5 or SHA is used, every bit of the message digest will depend on every bit of the original image.

The SHA-512 compression function operates on a 1024-bit message block and a

The SHA-512-bit compression function operates on a 1024-bit message block and a 512 bit intermediate hash value. It is essentially a 512-bit block cipher algorithm which encrypts the intermediate hash value using the message block as key. Hence there are two main components to describe: (1) the SHA-512 compression function, and (2) the SHA-512 message schedule.

5. Experimental Results

 # Result 1: Generic Visible Watermark Embedding

Input: an image I and a watermark L

Output: watermarked image W

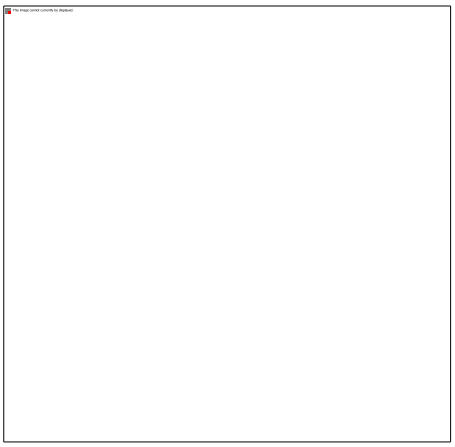

Fig.1 Generic Visible Watermark

Result 2: Generic Watermark Removal for Lossless Image Recovery

Input: a watermarked image W and a watermark L.

Output: the original image R recovered from W.

Fig.2 Lossless recovery of original image

#Result 3: Watermark Embedding of a Translucent Color Watermark

Input: an image I, a translucent watermark L

Output: : a watermarked image W

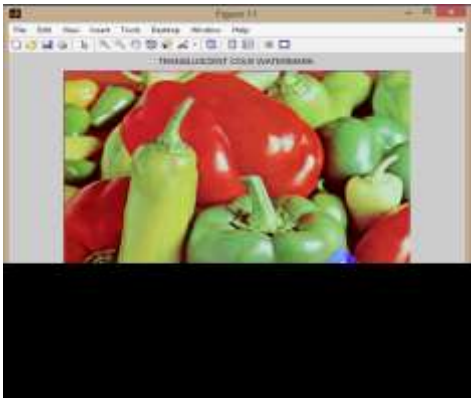

Fig.3 Embedding of Translucent color watermark

 # Result 4: Security Protection Based on Key using Hash Algorithm

Input: an image I , watermark L& Key K using Hash

Output: watermarked image W

Fig.4 Generic Visible Watermark based on Hash Algorithm

6. Conclusion

The lossless recovery of the watermarked image is exactly similar to the original image by using the one to one compound mapping. Hence we get the pixel by pixel similarity between the original image and the watermarked image after removing the watermark from the watermarked image. Also by using the Hash algorithm the watermark extraction will be depend on the secret key generated by the creator and only known to the intended receiver, hence only legitimate users can remove the watermark.

References

1. F.A.P. Petitcolas , R. J. Anderson, and M. G. Kuhn, " Information hiding —A survey," Proc. IEEE, vol. 87, no. 7, pp. 1062–1078,Jul.1999.
2. N. F. Johnson, Z. Duric, and S. Jajodia, Information Hiding. Steganography and Watermarking Attacks and Countermeasures. Boston, MA: Kluwer, 2001
3. I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673–1687, Jun. 1997.
4. M. S. Kankanhalli, Rajmohan, and K. R. Ramakrishnan, "Adaptive visible watermarking of images," in Proc. IEEE Int. Conf. Multimedia Computing and Systems, 1999, vol. 1, pp. 568–573.
5. Y. Hu and S. Kwong," Wavelet domain adaptive visible watermarking," Electron. Lett., vol. 37, no. 20, pp. 1219–1220, Sep. 2001.
6. S. P. Mohanty, K. R. Ramakrishnan, and M. S. Kankanhalli, "A DCT domain visible watermarking

technique for images," in Proc. IEEE Int. Conf. Multimedia and Expo, Jul. 2000, vol. 2, pp. 1029–1032.

7. G. Braudaway, K. A. Magerlein, and F. Mintzer, "Protecting publicly available images with a visible image watermark," in Proc. SPIE Int. Conf. Electronic Imaging, Feb. 1996, vol. 2659, pp. 126–133.

8. Y. J. Cheng and W. H. Tsai, "A new method for copyright and integrity protection for bitmap images by removable visible watermarks and irremovable invisible watermarks," presented at the Int. Computer Symp.—Workshop on Cryptology and Information Security, Hualien,Taiwan, R.O.C., Dec. 2002.

9. P. M. Huang and W. H. Tsai, "Copyright protection and authentication of grayscale images by removable visible watermarking and invisible signal embedding techniques: A new approach," presented at the Conf. Computer Vision, Graphics and Image Processing, Kinmen, Taiwan,

R.O.C., Aug. 2003.

10. Y. Hu, S. Kwong, and J. Huang, "An algorithm for removable visible watermarking," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no.1, pp. 129–133, Jan. 2006.

11. Y. Hu and B. Jeon, "Reversible visible watermarking and lossless recovery of original images," IEEE Trans. Circuits Syst. Video Technol.,vol. 16, no. 11, pp. 1423–1429, Nov. 2006.

12. B. Macq, "Lossless multiresolution transform for image authenticating watermarking," presented at the European Signal Processing Conf., Tampere, Finland, Sep. 2000.

13. J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding—New paradigm in digital watermarking," J. Appl. Signal Process., vol. 2002,no. 2, pp. 185–196, Feb. 2002.

14. M. Awrangjeb and M. S. Kankanhalli, "Lossless watermarking considering the human visual system," presented at the Int. Workshop on Digital Watermarking, Seoul, Korea, Oct. 2003.

15. M. Awrangjeb and M. S. Kankanhalli, "Reversible watermarking using a perceptual model," J. Electron. Imag., vol. 14, no. 013014, Mar. 2005.

16. C. de Vleeschouwer, J. F. Delaigle, and B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," IEEE Trans. Multimedia, vol. 5, no. 1, pp. 97–105, Mar. 2003.

17. J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

18. H. M. Tsai and L. W. Chang, "A high secure reversible visible watermarking scheme," in Proc. IEEE Int. Conf. Multimedia and Expo, Beijing, China, Jul. 2007, pp. 2106–2109.

19. S. K. Yip, O. C. Au, C. W. Ho, and H. M. Wong, "Lossless visible watermarking," in Proc. IEEE Int. Conf. Multimedia and Expo, Jul. 2006, pp. 853–856.

20. A. Lumini and D. Maio, "Adaptive positioning of a visible watermark in a digital image," in Proc. Int. Conf. Multimedia and Expo, Taipei, Taiwan, R.O.C., Jun. 2004, pp. 967–970.

21. X. Li and M. T. Orchard, "Edge-directed prediction for lossless compression of natural images," IEEE Trans. Image Process., vol. 10, no. 6, pp. 813–817, Jun. 2001.

22. Tsung-Yuan Liu and Wen-Hsiang Tsai , "Generic Lossless Visible Watermarking- A New Approach ," IEEE Trans. Image Process., vol. 19, no.5, May 2010

23. http://watermarkingworld.com

24. Shay Gueron, Simon Johnson &Jesse Walker, "SHA-512/256," Intel Architecture Group, Intel Corporation, USA , Department of Mathematics, University of Haifa, Israel

Author Profile

Mrunali Bhaisare received the B.E degrees in Electronics and Telecommunication Engineering from Mumbai University in 2012.

Currently persueing ME degree in Electronics and Telecommunication Engineering from PRMIT&R Badnera, Amravati University (2013-2015).