ijecs
open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 7 July 2017, Page No. 21982-21985
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i7.14

A Secure and Reversible Watermarking using Secret-Fragment-Visible Mosaic Images and Arnold's Cat map

Megha C. Bute, Prof. Shafali Gupta

Department of Computer Engineering
RMD Sinhgad School of Engineering, Pune, India
rasshmi21@gmail.com
Department of Computer Engineering
RMD Sinhgad School of Engineering, Pune, India
shafaligupta22@gmail.com

Abstract— **The image watermarking techniques are specially used to provide copyright protection, owners identification, image authentication and tamper detection. Water-marking technique is required to secure data and prevent unauthorized modification. The security and prevention from unauthorized modifications is due to rapid development of digital technologies, internet technologies and powerful image processing tools. Reversible watermarking becomes a promising technique to embed the information into important images. In this paper, we define the Region of Interest in an image and try to embed the data in Region of Non Interest. A basic idea of reversible watermarking is to select an embedding area in an image, embed the information into it and then rediscover the original image and information. If the amount of information need to embed is larger than embedding area, most of the techniques will consider lossless compression on the original values in the embedding area, and the space saved from compression will be used for embedding the watermark.**

Keywords— Reversible Watermarking, Region of interest, Region of non interest, Arnold's transform,Mosaic image

Introduction

Image watermarking techniques are specially used to provide copyright protection, owner's identification, image authentication and tamper detection. Due to the development of digital technologies and internet technologies, a large amount of digital data can easily be accessed via different transmission channels. Watermarking technique is used to prevent these modifications by embedding a watermark into the host image.

Watermark is an invisible signature embedded inside an image to show authenticity or proof of ownership. It discourages unauthorized copying and distribution of images over the internet and also ensures a digital picture has not been altered. The embedding technique can be visible - invisible, spatial - domain or transformed domain, robust or fragile. Reversible watermarking becomes a promising technique to embed the information into medical images as medical image content authentication and its recovery is very important. A new secure image watermarking method has been proposed, which not only can create meaningful mosaic images but also can transform a secret image into a mosaic one with the same data size for use as a camouflage of the secret image. By the use of proper pixel color transformations in the converted values of the pixels colors, secret-fragment visible mosaic images with very high visual similarities to arbitrarily-selected target images can be created with no need of a target image database. Also, the original secret images can be recovered nearly lossless from the created mosaic images. The research shows that the robust encryption technique has to be developed which will secure the data and prevent it from unauthorized manipulation. The proposed system solves this problem by using two different watermarking algorithms, mosaic image generation and then applying cap map technique.

REVIEW OF LITURATURE

Digital image watermarking techniques have been developed widely in recent years to maintain content authentication and broadcasting media, broadcast monitoring, copy control, and many other applications[5]. Digital image watermarking is the technique to embed a host image with the to be watermark, then the watermarked image will be transferred, and the secret image can be extracted at the receiver. First use of watermarks can be trace back to paper mills in Italy to authenticate there product Since then the are common in print industries and used by various commercial and government organization due to their uses. In particular conditions Digital watermarking has similarities steganography with main difference is that in steganography the hidden data is more important while in digital watermarking both hidden and host data is important.

Most of the Digital image watermarking techniques have been developed widely in recent years for maintaining the broadcasting media and content authentication, broadcast monitoring, copy control, and many other applications.

Properties of a digital watermark depend on the use case in which it is applied, therefore Robustness ,Imperceptibility ,Security and capacity are some properties that should give characteristics of a watermark [6].

The watermark is developed to be able to survive against incidental and intentional attacks. This robust kind of watermarking can be used in broadcast monitoring, copyright protection, fingerprinting, and copy control[8]. A digital watermark can be called as "fragile" watermark if it fails to be detectable after the slightest modification. Fragile watermarking techniques are commonly used for tamper detection (integrity proof). semi-fragile watermark resists simple transformations, but fails detection complex transformation. Semi-fragile watermarks commonly are used to for content authentication.

The term Imperceptibility can be referred to as the perceptual similarity between the original image before watermarking process and the watermarked image, i.e. if the watermark is visible or not. Security is the ability to resist against intentional attacks and in last Capacity (also known as Payload) refers to the number of bits embedded into the image. Capacity can be also be defined as the limit to which the watermark could be embedded in the host image[6].

The watermarking techniques are also classified in two types spatial domain and transform domain. In Spatial domain information is directly inserted into the image. Transform Domain embedding uses the transform coefficients to embed the watermark .The special domain techniques are bit manipulation such as LSB and ISB. The bit manipulation techniques does not cause visible changes in the image. The transformation techniques examples are DCT and DWT .This type of embedding uses the transform coefficients to embed the watermark. Moreover, transform domain techniques are very robust against attacks, because the watermark is spread in whole image [9]. Recently Fragile watermarks are used to locate the tampered areas when the image has been tampered. Recently many fragile watermarking schemes for content authentication, integrity verification and for image tamper detection have been proposed[10] by using both spatial and transformation domain techniques.

DISTORTIONS AND ATTACKS

First of all, we have to distinguish two “reasons” or “purposes” for an attack against a watermark image:

Hostile or malicious attacks, which are an attempt to weaken, remove or alter the watermark, and Coincidental attacks, which can occur during common image processing and are not aimed at tampering with the watermark. Lossy image compression is considered the most common form of attack a watermarking scheme has to withstand. The harsh term “attack” can be easily justified: an efficient image compression has to suppress or discard perceptually irrelevant information the invisible watermark. A wide range of attacks has been described in the literature . The following four large categories of attacks can be invoked to penetrate a watermarking system:

- Removal attacks
- Geometrical attacks
- Cryptographic attacks
- Protocol attacks

PRACTICAL ENVIRONMENT

Hardware :
Processor : Pentium IV
RAM : 512MB DD RAM
Monitor : 15 color
Hard disk : 20 GB
Keyboard : Standard 102 keys
Mouse : 3 buttons
Software :NetBeans IDE
Front end : Java
Back end : JDBC
Operating system : Windows 7/XP

MATHEMATICAL MODEL

A) Creation of mosaic image Im={Or_im, Tr_im} where Or_im is the original image that is secret and Tr_im is the target image in which it is to be embedded .

Output of this will be the mosaic image.

B) Retrieving the secret image Imr={Im, reverse_theorem()}

where Imr is secret image which is retrieved by reverse theorem.

C) Applying Arnold's cat map method for tamper detection Imr={Or_im, Imr, detect()}

where Or_im is the original secret image andImr is the retrieved secret image and detect is the function which detects tampering.

PROPOSED SYSTEM

The main goal is to secure the image by using watermark technique. The System will create a mosaic images for RGB, HSV as well as LAB models and do a comparative study of all the outcomes. Then our system should be able to reverse the technique to get the original image.

In the first phase, a mosaic image is yielded, which consists of the fragments of the secret image which is input with color corrections according to a similarity criterion based upon color variations. In the second phase, the secret image will be retrieved using the reverse theorem and tamper detection will be done by using Arnold’s cat map method. The embedded information will then be extracted to recover nearly lossless secret image from the generated image.

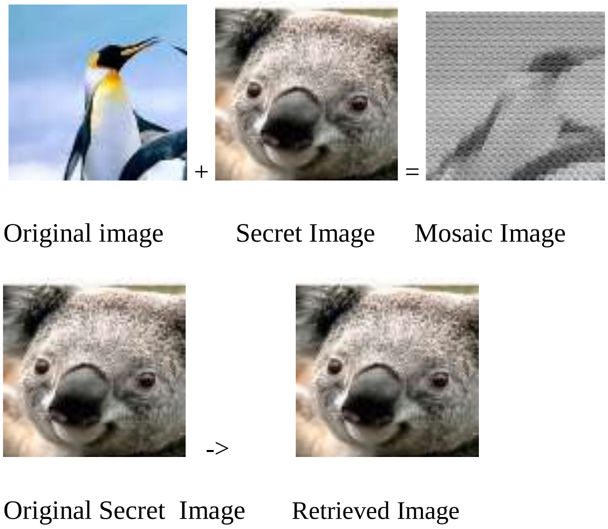

Fig. 1. Proposed outcome

APPROACH TO GET THE OUTCOME

The below given approach will be followed to get the outcome as shown in the *fig. 1.* There will be 3 steps in which the system will be divided.

1. Creation of the mosaic image :

In the first phase, a mosaic image I yielded, which consists of the fragments of secret image with color corrections according to a similarity criterion which is here based upon color variations. The phase includes four stages first fitting the tile images of the secret image into the target blocks of a preselected target image; then transforming the color characteristic of each tile image in the secret image to become that of the corresponding target block in the target image; and rotating each tile image into a direction with the minimum RMSE value with respect to its corresponding target block; At last embedding relevant information into the created mosaic image for future recovery of the secret image.

2. Recovering of the Secret image :

In the second phase, the watermarked information is then extracted to recover nearly lossless the secret image from the generated mosaic image. The phase includes two stages; one is extracting the embedded information for secret image recovery from the mosaic image, and the second is recovering the secret image using the extracted information.

3. Applying cat map watermarked image:

As the security is the major concern as well as point of attention for watermarking algorithms, chaotic maps generate chaotic image pattern for increasing the security. These types of maps are sensitive to initial conditions. Two dimensional Arnold cat map shuffles the pixels positions of the original image without changing the pixels gray level intensities.

Outcomes
Our model can create a highly secure image by using watermarking techniques and similarly can extract the original image by reversible technique.

ALGORITHM

A)Creation of the Mosaic image
Fitting tile images into the target blocks.

1. If the size of the target image *T is different from* that of the secret image *S, change the size of T to be* identical to that of *S; and divide the secret image S* into *n tile images {T1, T2, . . . , Tn} as well as the* target image *T into n target blocks {B1, B2, . . . , Bn}*

with each *Ti or Bi being of size NT .*

2. Compute the means and the standard deviations of each tile image Ti and each target block Bj for the three color channels compute accordingly the average standard deviations for Ti and Bj , respectively, for i = 1 through n and j = 1 through n.

3. Sort the tile images in the set *Stile = {T1, T2, . . . ,Tn} and the target blocks in the set Starget = {B1,B2, . . . , Bn} according to the computed average* standard deviation values of the blocks; map in order the blocks in the sorted *Stile to those in the sorted Starget in a 1-to-1 manner;* and reorder the mappings according to the indices of the tile images, resulting in a *mapping sequence L of the form: T1 → Bj1 , T2→ Bj2 , . . . , Tn → Bjn .*

4. Create the required mosaic image F by fitting the tile images into the corresponding target blocks according to L.

Perform the color conversions between the tile images and the target blocks.

5. Create a counting table TB with 256 entries, each with an index corresponding to a residual value, and assign an initial value of zero to each entry (note that each residual value will be in the range of 0 to 255).

6. For each mapping Ti →Bji in sequence L, represent the means μc and μ c of Ti and Bji, respectively,by eight bits; and represent the standard deviation quotient qc by seven bits, according to the scheme described in Section III(A) where c = r, g, or b.

7. For each pixel pi in each tile image Ti of mosaic image F with color value ci where c = r, g, or b,transform ci into a new value ci ; if ci is not smaller than 255 or if it is not larger than 0, then change ci to be 255 or 0, respectively; compute a residual value Ri for pixel pi by the way described in Section III(C); and increment by 1 the count in the entry in the counting table TB whose index is identical to Ri.

B)Applying Arnold's Cat map
1. Firstly, the scrambled image Fscr is obtained from the mosaic image F using Arnold cat map. The scrambled image is obtained from the mosaic image after K times iterations of cat map. Here K acts as a secret key.

2. After obtaining the scrambled image, the scrambled image is divided into 8-bit planes. In other words, 8-bits are extracted from each pixel of the scrambled image.

3. From the scrambled image check sum is calculated using exclusive-or (XOR) operator of 8-bits of each pixel.

4. A binary image is considered as the watermark image whose size should be equal to the size of the original image. The pixels of the watermark image are compared with check sum or XOR results one by one.

(i) The pixels of the scrambled image are unchanged if the values of watermark pixels are same as the values of XOR results.

(ii) The pixels of scrambled image are being modified by changing the Least Significant Bits (LSB) if the values of watermark pixels are not same as the values of XOR results.

```
if ( W(x, y) is not equal XOR(x, y) )

{

LSBm(scr)(x, y) = LSBscr(x, y) + 1 ; if LSBscr(x, y)=0

LSBm(scr)(x, y) = LSBscr(x, y) - 1 ; if LSBscr(x, y)=1

}
```

Where, LSBscr is the least significant bit plane of scrambled image and LSBm(scr) is the modified least significant bit plane of scrambled image.

Finally, the watermarked image can be obtained by applying (T-K) iterations on the modified scrambled image. Here T is the period of the cat map.

C) Extraction of the Mosaic image

Firstly, the scrambled watermarked image FWscr is obtained by using the correct key. Then 8-bits from each pixel of scrambled watermarked image are extracted. The check sum is calculated from FWscr by using XOR operator of 8-bits of each pixel. The check sum or XOR results give the watermark image that was embedded into the scrambled image.

RESULT

Proposed system is expected to produce the scrambled image after applying mosaic image creation and cat map algorithms. This system achieves high security in case of watermarked image processing. Two dimensional cat map will be used to scramble the image. Three secret keys are obtained for the proposed method. The watermark can be extracted from the watermarked image using the correct keys. By investigating the experimental results, it can be said that the proposed method gives low values of MSE and high values of PSNR compared to the existing methods in [8] which is required for image watermarking. The proposed method also gives low value of EBR compared to the existing methods in [8] .This proves the robustness of the proposed

method.

Module 1:

It contains basic GUI design with database design of required tables of fields. We will take an image which is to be watermarked, then process it by encoding another image. The output of this module will be mosaic image.

Module 2:

It contains recovering of the secret image using reverse theorem. This module will extract the secret image which is hidden inside the mosaic image.

Module 3:

This will include tamper detection where concept of xor'ing the bits from Arnold's cat map method is used to detect tamper in extracted secret image.

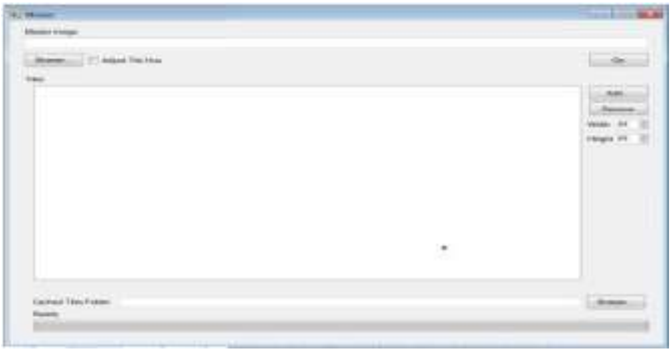

Fig. 2 UI design

CONCLUSION AND FUTURE WORK

A new secure image transmission method has been proposed, which not only can create meaningful mosaic images but also can make it more secure and reversible with the help of two dimensional Arnold's cat map.

Future scope may be directed to image tamper detection and applying the proposed method to images of color models other than the RGB.

ACKNOWLEDGMENT

I take this chance to express my appreciation to my guide Prof. Shafali Gupta Department of Computer Engineering,

RMD Sinhgad School of Engineering, Pune, India ,for their kind cooperation and guidance during the entire research work. I would also like to thank our, Principal and Management for providing lab and other facilities.

REFERENCES

[1] A New Secure Image Transmission Technique via Secret-Fragment-Visible Mosaic Images by Nearly Reversible Color Transformations, Ya-Lin Lee, and Wen-Hsiang Tsai, Senior Member, IEEE Tran.Vol. 24, no. 4, April2014.

[2] Gouenou Coatrieux,Clara le Guillou,J.Cauvin and Ch,Roux:"Reversible watermarking for knowledge digest embedding and reliability control in medical images',IEEE Transaction on information technology in biomedicine, vol.13,No.2,March 2009.

[3] G.Coatrieux, M.lamard, WDaccache, j.Puentes, and C.Roux,"A low distortion and reversible watermark application in angiographic images of the retina," in proc.lEEE-EMBC,Shanghai, China, 2005, pp. 2224-2227.

[4] W.Pan,G.Coatrieux,N.Cuppens-Boulahia,F.Cuppensand Ch.Roux:"medical image integrity control combining digital signature and lossless watermark-ing", published in 2nd SSETOP international workshop on autonomous and spontaneous security, Saint Malo: France, 2009, Version 1-14 Jan 2010.

[5] Micheal W.Marcellin, micheal J.Garmish, Ali Bilgin and Martin p.bolick,"An overview of JPEG-2000," in proc IEEE data compression conference, pp.523-541, 2000.

[6] I. Cox and M. L. Miller. A review of watermarking and the\importance of perceptual modeling. I Proceedings of SPIE, Human Vision & Electronic Imaging II, volume 3016, page 92–99, 1997

[7] Changjiang Zhang et al. , "Digital Image watermarking with Double encryp tion by Arnold Transform and Logistic ", Fourth International conference on Networked Computing and advanced information Management, pp. 329-334,2008.

[8] C.Y.Lin and S.F.Chang.: A robust image authentication method distinguishing jpeg compression from malicious manipulation, IEEE Trans. On Circuits and Systems of Video Technology, 11:153{168, Feb. 2001.}

[9] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process., vol. 13, no. 4, pp. 600–612, Apr. 2004.*

[10] S. Jun and M. S. Alam, "Fragility and Robustness of Binary-Phase-Only-Filter-Based Fragile/Semifragile Digital Image Watermarking," *Instrumentation and Measurement, IEEE*Transactions on, vol. 57,