Multiuser Watermarking using Visual Cryptography

Komal Toshniwal
M.E.Student, D.Y.Patil, Pimpri, Pune

Prof.Santosh Chobe
HOD (IT Dept.)
D.Y.Patil, Pimpri, Pune

Abstract: Watermarking is a technique to protect the copyright of digital media such as image, text, music and movie. In this study, a robust watermarking scheme for multiple cover images and multiple owners is proposed. the rest of the techniques are applied to enhance the robustness of the scheme. This technique will help many internet users to embed the watermark in their photos before uploading them to common social networking sites like "Facebook" or "Orkut" or "Flicker" to avoid misuse of their uploaded photos

Keywords: Stenography, Permutation, Visual Cryptography,

I. INTRODUCTION

With the rapid development of the internet, the transferring of digital media over the internet becomes increasingly popular. Hence, the copyright protection of digital media becomes a hot topic since the digital media can be obtained and distributed easily over the internet. In this paper, we will focus on watermarking schemes for digital images. Generally, a watermarking scheme combines cover images with a watermark that is hard to be detected and removed, and the owner of the image can prove his copyright by extracting the watermark from the watermarked image. Generally, a watermarking scheme should meet several criteria, such as imperceptibility, robustness, security and blindness. Visual cryptography (VC)-based watermarking schemes have been proposed in recent years. The advantages of VC technique for watermarking are that: first, it can achieve large embedding capacity, that is, it can embed a large watermark (an image) into the cover images;

second, it can achieve high security; third, it has the ability to share a secret image between multiple users. However, its robustness is a disadvantage.

In this paper, in order to enhance the robustness of the VC-based watermarking schemes, the transform domain technique, chaos technique, noise reduction technique and error correcting code technique are applied. For most VC-based watermarking schemes in the literature, each cover image corresponds to a secret image that is registered to a trust authority (TA). Note
that, an owner may have the copyright of multiple images. If only generate one secret image for all the images he owns, it will reduce the burden of TA significantly. Furthermore, besides the case that an owner owns multiple images, there may be the case that, an image is owned by multiple owners, which may be caused by several reasons, for example, the image is created by multiple photographers collaboratively.
Digital watermark is used to extend the protection and provide the opportunities for the content owners to protect the rights and properties of the electronic distributed contents. The signature of the owner, content ID and usage limitation can be imprinted into the contents, and stay with the contents as far as it travels. This mechanism extends the opportunity of protecting the contents after the release of the contents to the open environment.
The major technical requirements for this application are as follows:

- The watermark does not incur visible (or audible) artifacts to the ordinary users.
- The watermark is independent of the data format.
- The information carried by the watermark is robust to content manipulations, compression, and so on.
- The watermark can be detected without the un-watermarked original content.
- The watermark can be identified by some kind of "keys" that are used to

- identify large number of individual contents uniquely.

The material that contains a digital watermark is called a carrier. A digital watermark is not provided as a separate file or a link. It is information that is directly embedded in the carrier file. Therefore, the digital watermark cannot be identified by simply viewing the carrier image containing it. Special software is needed to embed and detect such digital watermarks.

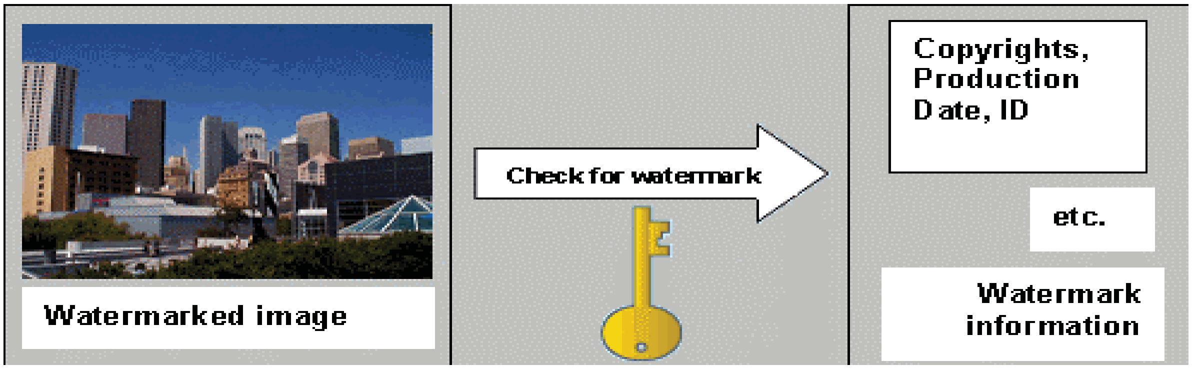


Figure **Error! No text of specified style in document.**-1 Structure of digital watermark

1.1 Purpose

The purpose of the project is related to Watermarking of pictures, media, videos shared by multiple owners using Visual cryptography. This SRS section describes the functions and performance requirements for Watermarking of pictures, media, videos shared by multiple owners using Visual cryptography. Visual cryptography is used for embedding the water mark image and multiple key images and creates a share that can be registered with Trusted Authority (TA).

1.2 Overall Description

For this section of the document; we first of all have defined the overall product. Then, we have given the external interface requirements, followed by a brief description of the product components and features. In the last section, we have provided the non functional requirements of the product.

- The model of this scheme includes three kinds of participants
  - the owners of the cover images who want to protect their copyright of the cover images
  - the attackers who want to illegally use the cover images
  - A TA who will arbitrate the ownership of the cover images when a dispute occurs.
- It is assumed that, t owners own n images, and there is only one TA
- The proposed watermarking scheme contains two algorithms
  - The embedding algorithm
  - The extracting algorithm.

II. SYSTEM FEATURES

Generally, a watermarking scheme should meet the following criteria:

- **Imperceptibility**: It is hard to detect the differences between the original cover images and the watermarked ones by the human visual system. The imperceptibility is perfect if the watermarked images are identical / indistinguishable to the original cover images.
- **Robustness**: The watermark still can be extracted even the watermarked image suffers from various attacks.
- **Security**: Only the owner of the cover images can extract the watermark from the watermarked image.
- **Blindness**: The original cover images are not required for extracting the watermark. Hence, extra space is not required for storing the cover images. Currently, most of the watermarking schemes are based on the transform domain techniques.

Following techniques are used to enhance the robustness of copyright for multiuser for their cover image.

- Visual cryptography

- Torus auto-morphism
- Discrete wavelet transform
- Error correcting technique

Following are the techniques which are used by the system to achieve the encryption and decryption of the images.

2.1 Visual Cryptography

VC is a kind of technique to share secret images. We apply this technique to protect the owners' copyrights of the cover images. Generally speaking, a (k, n)-VCS takes a secret image as input, and outputs n share images that satisfy two conditions first, any k out of n shares can recover the secret image; second, any less than k shares cannot get any information about the secret image (unconditionally secure).

The underlying operation of the VCS is XOR (exclusive-OR). In this scheme, we make use of the VCS with underlying operation XOR, because an XOR-based VCS usually has better performance in terms of the visual quality of the recovered secret image and the pixel expansion. An example of (2, 2)-VCS with underlying operation XOR is shown in below Fig denote □ as the XOR operation, we have (d) = (b) □ (c)

2.2 Chaos Technique

The chaos technique is widely used in the study of watermarking. A famous and simple chaos technique is the torus automorphism. Its transformation is defined by the following formula

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \bmod N$$

where (xi, yi) and (xi+1, yi+1) are the coordinates of pixels in an image, i is the number of rounds of the torus automorphism, and N × N is the size of the image. The pixel at position (x1, y1) is moved to the position (xi, yi) after i rounds of the torus automorphism. The inversion of torus automorphism exists since

$$\det\begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} = 1.$$

The model of watermarking can be viewed as an information transmission model, where the cover image is the channel and the watermark is the message. The attacks of the watermarking scheme add error pixels (noise) to the watermark (message). For some attacks, the error pixels may be aggregated, for example, the cropping attack.

The torus automorphism can scatter the error pixels to the entire image uniformly. Take the cropping attack with 25% of the cover image being cropped as an example, after the torus automorphism process, there is on average one error pixel in each four pixels, and hence we may have a chance to correct the error pixel by the information of the remaining three correct pixels.

2.3 Error Correcting Code Technique

The attacks of the watermarking scheme add errors (noise) to the watermark (message). Hence, it is natural for us to use the error correcting code technique to reduce the errors. In this paper, use of (8, 2, 5) Cordaro–Wagner Code, where the code length is 8, with two information bits and the minimum distance between the codes is 5. The (8, 2, 5) Cordaro–Wagner Code is

maximum distance separable (MDS) code that can correct two errors.

The four code words of (8, 2, 5) code are as follows {00000000, 10110111, 01001111, 11111000} Note that there are many kinds of MDS error correcting codes. One reason that (8, 2, 5) Cordaro–Wagner Code used is that this code can correct (2/8) = 25% errors which is comparable to the 25% cropping attack

2.4 Transform domain technique

The transform domain technique can extract the feature image of the cover image; hence, watermarking schemes based on the transform domain technique often have strong robustness against compression attacks. In this paper the two-level DWT will be used (Discrete Wavelength Transform), where the decomposition of an image by using two-level DWT.

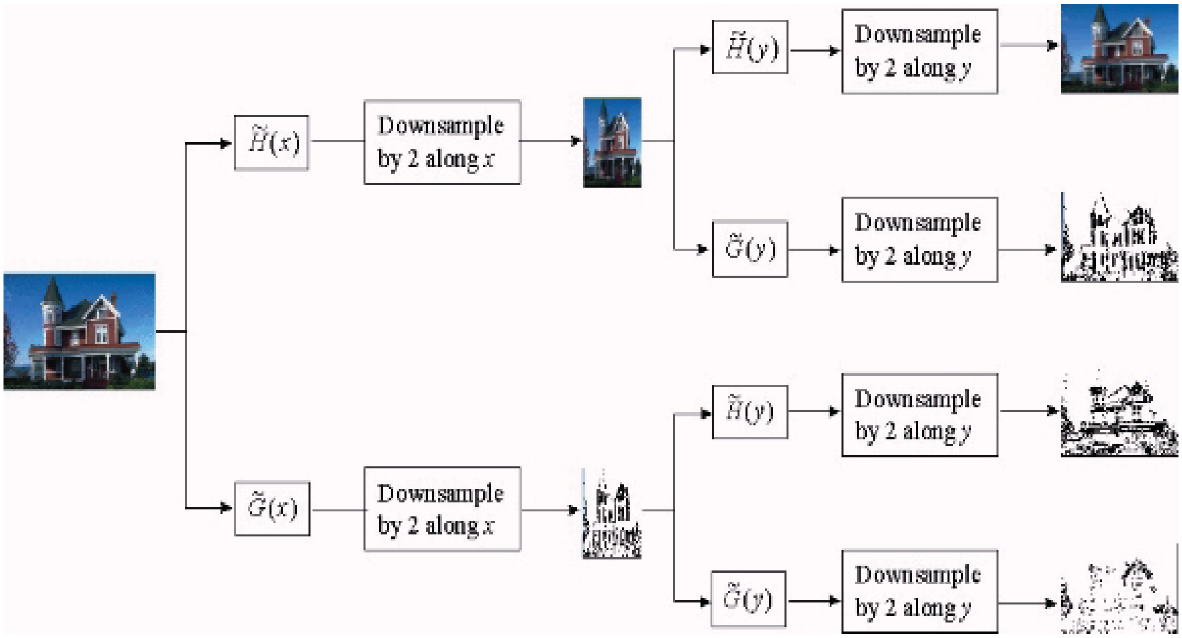

$\tilde{H}(x)$
Downsample by 2 along x
$\tilde{H}(y)$
Downsample by 2 along y
$\tilde{G}(y)$
Downsample by 2 along y
$\tilde{G}(x)$
Downsample by 2 along x
$\tilde{H}(y)$
Downsample by 2 along y
$\tilde{G}(y)$
Downsample by 2 along y

Figure 2-2 High Pass and Low Pass Filters for 2 level DWT

By using the two-level DWT, the original image is firstly decomposed into four sub-bands that are normally labeled as LL1, LH1, HL1 and HH1. The LL1 sub-band is further decomposed into four sub-bands labeled as LL2, LH2, HL2 and HH2.The LL sub-band comes from low-pass filtering in both directions and it looks most like the original image. The LL sub-band contains most of the information of the original image.

The remaining sub-bands are called detailed components. The sub-bands LH, HL and HH represent horizontal, vertical and diagonal details, respectively.

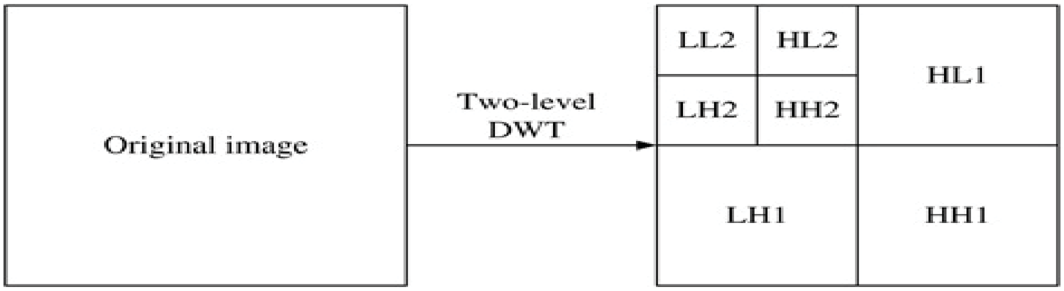


Figure2-2 Level DWT

III. Software Quality Attributes

- Correctness:
    - The system works correctly and efficiently if it is used in
    - the way mentioned in the user manual.
    - Any user who behaves erratically with the system is bound to cause the system to react in an unusual manner.
    - The correctness of the system depends on the way it is handled.
    - The accuracy of the system is limited by the accuracy of the speed at which the Employees of the system and users of the use the system.
- Maintainability

  - The system is easy to maintain and the annual maintenance of the system shall be done as per the maintenance contract.
  - Regular maintenance of the system is essential for ensuring the system gives optimal performance.
- Portability
  - The system can be easily installed on any valid configuration and is easily
  - portable. However to ensure stable performance it is recommended that the system be installed at one location permanently.

3.1 ALGORITHMS

3.1.1 The embedding algorithm

- **Input:** n cover images I1, . . . , In and a watermark image W.
- **Output:** The watermarked images, a secret share S that is registered to TA and t key images K1, . . . , Kt that are distributed to the owners.
- **Step 1:** Apply two-level DWT to obtain the feature images of the cover images FI1, . . , FIn, where FI1, . . . , FIn are the low sub-band LL2 of the cover images I1, . . . , In, respectively.
- **Step 2:** Convert the feature images FI1, . . ., FIn into binary images BI1, . . ., Bin . The conversion can be realised by setting a threshold d, and the pixels with grey values that are larger than d are set to 1, the rest are set to 0.
- **Step 3:** Convert the watermark image W into a chaotic image WT by applying the torus automorphism with parameter k for i rounds.
- **Step 4:** Encode the chaotic image WT into WE by using the (8, 2, 5) Cordaro–Wagner Code.
- **Step 5:** Generate t random key images K1, . . . , Kt for t owners,where the size
- of each key image is identical to the size of WE.
- **Step 6:** Generate the secret share S by applying the (n + t + 1,n + t + 1)-VCS based on XOR operation, $W_E = S \oplus \mathrm{BI}_1 \oplus \cdots \oplus \mathrm{BI}_n \oplus K_1 \oplus \cdots \oplus K_t,$ that is, where $S = W_E \oplus \mathrm{BI}_1 \oplus \cdots \oplus \mathrm{BI}_n \oplus K_1 \oplus \cdots \oplus K_t.$
- **Step 7:** Publish I1, . . . , In and W as the watermarked images and the watermark, register S to TA secretly and distribute K1, . . . , Kt to the owners secretly. The flow chart of the embedding algorithm

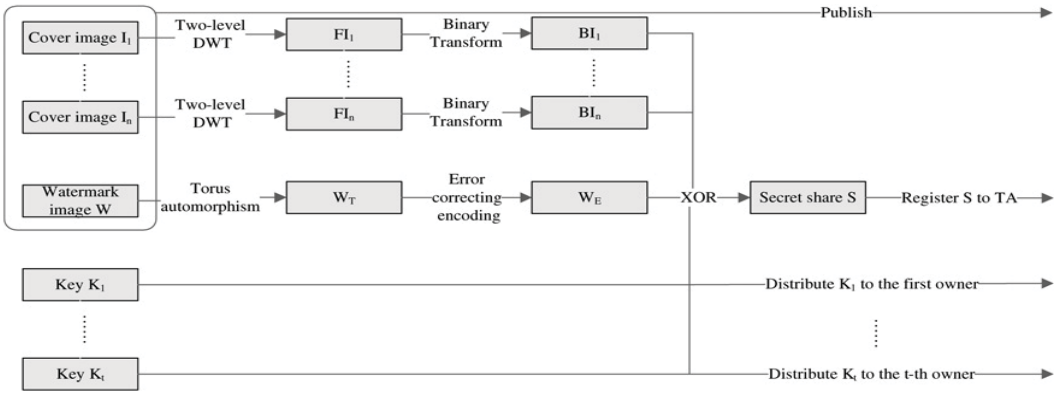


Figure3-1 Embedding Algorithm

3.1.1.1 Remark:

- In Step 3 of Algorithm 1, the parameters k and i can be kept private or public subject to security concerns. The security of the scheme is guaranteed by the security of VCS.
- Note that the key images K1, . . . , Kt are random images that are distributed to the owners secretly, that is, the attackers do not have any information about K1, . . . , Kt. The secret share S is generated by $S = W_E \oplus \mathrm{BI}_1 \oplus \cdots \oplus \mathrm{BI}_n \oplus K_1 \oplus \cdots \oplus K_t.$

- According to the security of VCS, because the attackers do not have K1, . . . , Kt, the attackers have no way to get any information about S either that is the attackers cannot claim the ownership of the cover images.
- Step 5 can also be realised by generating t keys (such as passwords), and by taking the t keys as seeds of a pseudorandom number generator, one also can generate t key images K1…Kt. In such a way, the owners only need to remember a password rather than to take a key image.
- Note that, by applying the XOR-based extended VCS proposed the key images
- K1… Kt and the secret share S can be meaningful images rather than noise like shares.
- According to the embedding algorithm, the watermarked images are identical to the cover images. Hence, the imperceptibility of our scheme is perfect.
- And it only generates one secret share for multiple cover images and multiple owners, and hence, it saves storage memory of the secret shares for TA.

3.1.2 *The extracting algorithm*

- **Input:** The attacked images I′1, . . . , I′n, the secret share S and t key images K1, . . . , Kt.
- **Output:** An extracted watermark image W′ ‘and compare it with the original watermark.
- **Step 1**: Apply two-level DWT to obtain the feature images of the attacked images FI′1…FI ′ n, where FI′1, . . ., FI
- ′n are the low sub-band LL2 of the attacked images I′1, . . . , I′n, respectively.
- **Step 2**: Convert the feature images FI′1, . . ., FI ′n into binary images BI′1, . . ., BI ′ n. The conversion method is the same as that of the embedding algorithm.
- **Step 3:** Obtain the secret share S from TA, and obtain the t key images K1, . . . , Kt from the owners.
- **Step 4:** Generate the W′ S by the following equation $W'_S = S \oplus BI'_1 \oplus \cdots \oplus BI'_n \oplus K_1 \oplus \cdots \oplus K_t$
- **Step 5:** Decode the W′S into W′E by using the (8, 2, 5) Cordaro–Wagner Code.
- **Step 6:** Generate W′T by applying the inversion of the torus automorphism.
- **Step 7:** Reduce the noise in W ′T by using a median filter to get the extracted watermark W′.
- **Step 8:** Compare the watermarks W and W′ by calculating the value of AR. The flow chart of the extracting algorithm is shown in Fig.

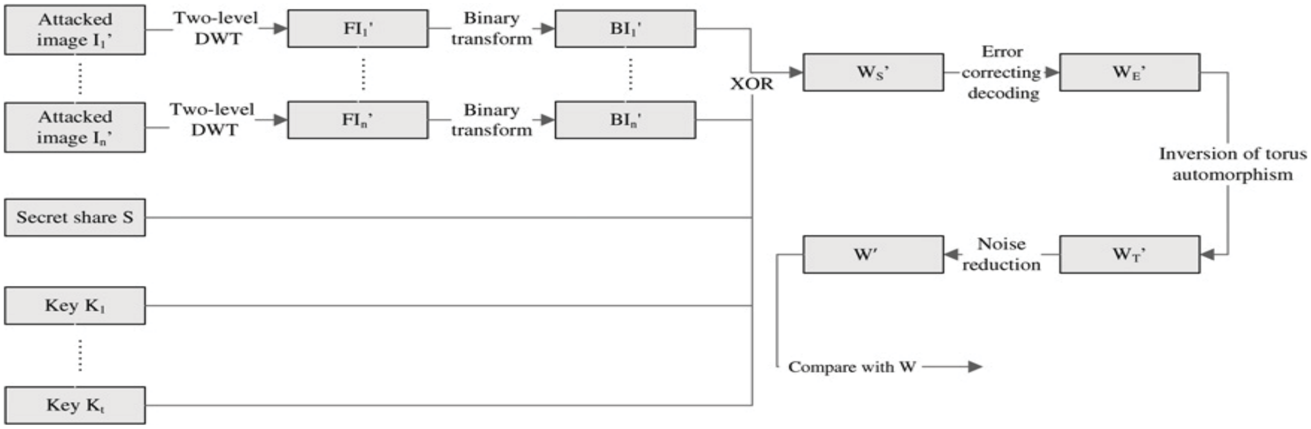
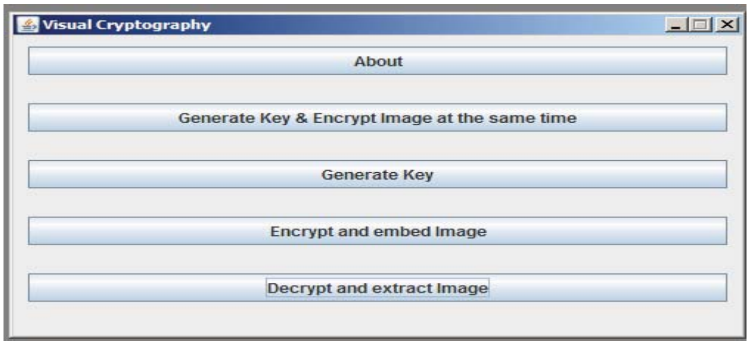
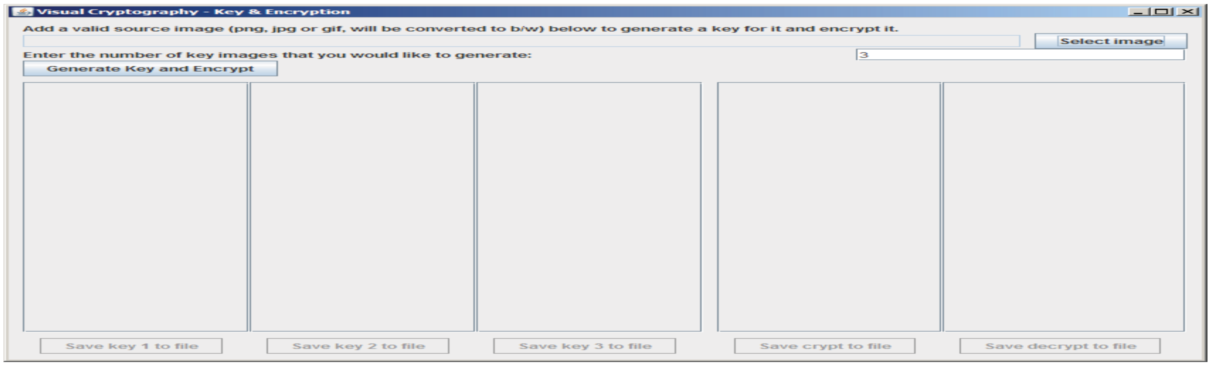


Figure3-2 Extracting Algorithm

IV. TECHNICAL SPECIFICATION


Visual Cryptography
About
Generate Key & Encrypt Image at the same time
Generate Key
Encrypt and embed Image
Decrypt and extract Image

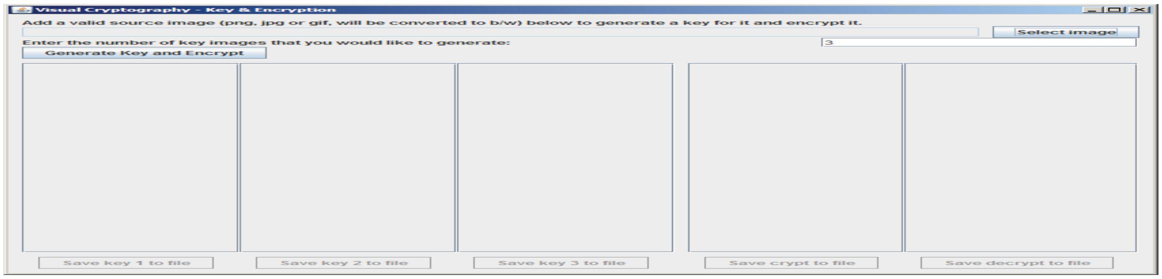


Add a valid source image (png, jpg or gif, will be converted to b/w) below to generate a key for it and encrypt it.

Enter the number of key images that you would like to generate: 3

4.1Generate Key & Encrypt at the same time

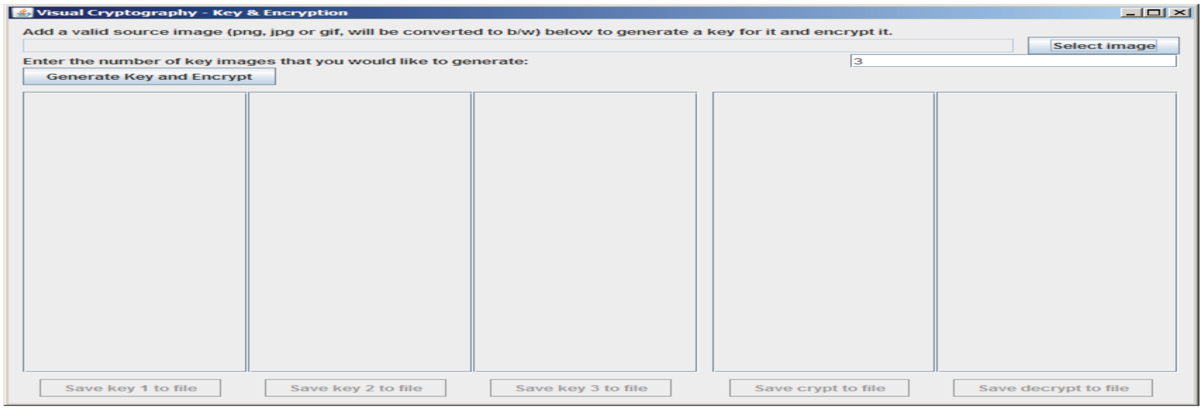
4.2 Generate Key



Add a valid source image (png, jpg or gif, will be converted to b/w) below to generate a key for it and encrypt it.

Enter the number of key images that you would like to generate: 3

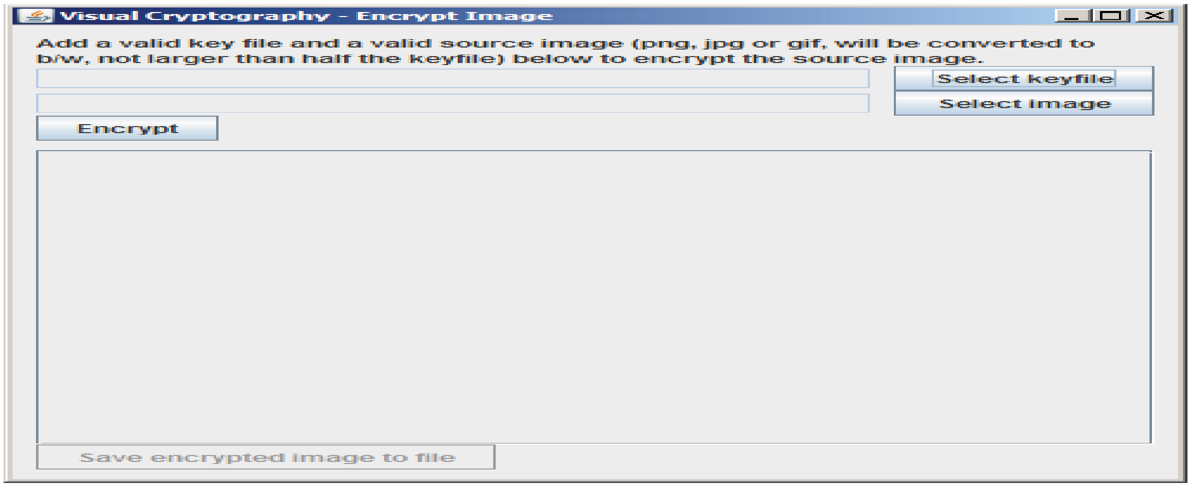
4.3 Encrypt and embed Image



Add a valid source image (png, jpg or gif, will be converted to b/w) below to generate a key for it and encrypt it.

Enter the number of key images that you would like to generate: 3

4.4Generate Key



Visual Cryptography - Encrypt Image

Add a valid key file and a valid source image (png, jpg or gif, will be converted to b/w, not larger than half the keyfile) below to encrypt the source image.

4.5 Encrypt and embed Image

In this paper

- a1 is the JPEG compression attacked image with qualify factor 5%
- a2 is the JPEG compression-attacked image with qualify factor 10%
- a3 is the blurring attacked image that is generated by using a averaging filter with parameter 11 on the cover image
- a4 is the sharpening-attacked image that is generated by using a multi-dimensional filter the cover image
- a5 is the scaling attacked image that is generated by reducing the cover image to size 64 × 64 and then enlarged to size 512 × 512
- a6 is the cropping attacked image with 10% of the cover image being cropped
- a7 is the cropping attacked image with 25% of the cover image being cropped
- a8 is the distortion attack that is generated by pinching and spherising the cover image
- a9 is the noising-attacked image that is generated by adding the salt and pepper noise with parameter 20%; r is a different image(s).

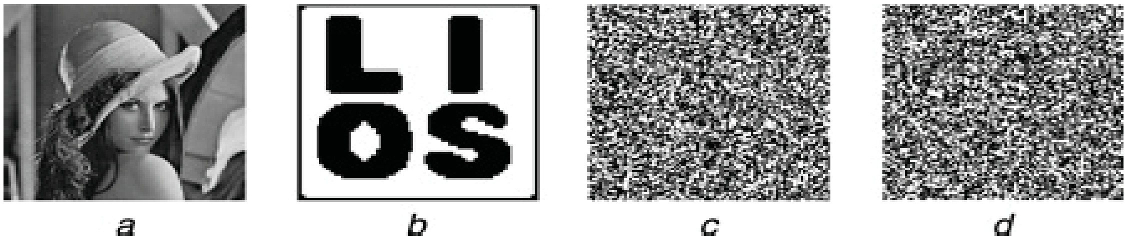
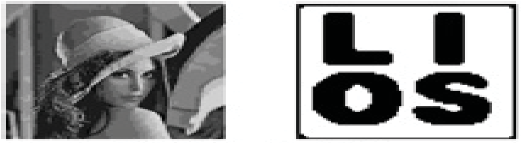
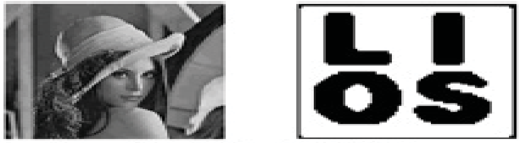


Figure 4-6Test images for the first simulation

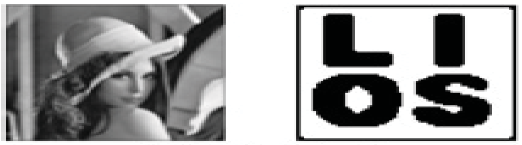
a-Cover image, b-Watermark, c-Key image, d-Secret share



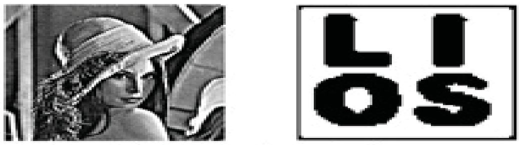
a1: JPEG attack 5%



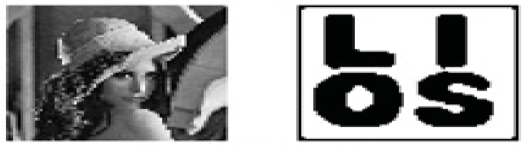
a2: JPEG attack 10%



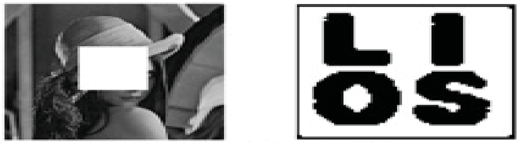
a3: blurring attack



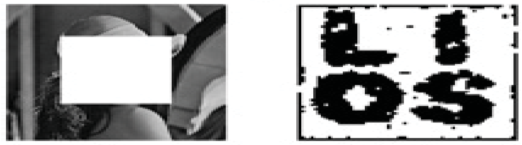
a4: sharpening attack



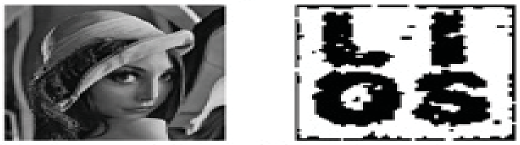
a5: scaling attack



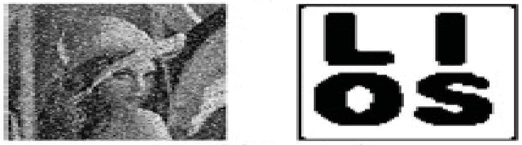
a6: cropping attack 10%



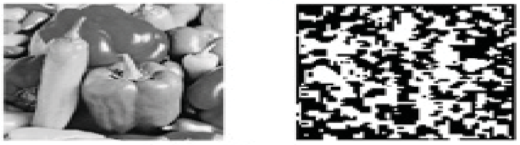
a7: cropping attack 25%



a8: distortion attack



a9: noising attack



a10: other image

V. CONCLUSION

In this paper, we proposed a VC-based watermarking scheme, which has strong robustness, perfect imperceptibility, and satisfies the blindness and security properties. Furthermore, the proposed scheme can deal with multiple owners and multiple cover images. A qualitative comparison on effectiveness between our scheme and some known VC-based watermarking schemes. The comparisons show that our scheme has many good properties. Also tiring to develop it for no of images of all the extantions.

REFERENCES

[1] Wang, F.H., Yen, K.K., Jain, L.C., Pan, J.S.: ‘Multiuser-based shadow watermark extraction system’, Inf. Sci., 2007, 177, pp. 2522–2532

[2] Lou, D.C., Tso, H.K., Liu, J.L.: ‘A copyright protection scheme for digital images using visual cryptography technique’, omput.Stand.Interfaces, 2007

[3] Hsieh, S.L., Hsu, L.Y., Tsai, I.J.: ‘A copyright protection scheme for color images using secret sharing and wavelet transformation’. Proc. World Academy of Science, Engineering and Technology, 2005

[4] Wang, M.S., Chen, W.C.: ‘Digital image copyright protection scheme based onvisual cryptography and singular value decomposition’, Opt.Eng., 2007

[5] Hsu, C.T., Wu, J.L.:‘Hidden digital wtermarks in images’, IEEE Trans. Image Process., 1999 Voyatzis, G., Pitas, I.: ‘Applications of toral automorphisms in image watermarking’. Proc. Int. Conf. on

[6] Image Processing, 1996, vol. 2, pp. 237–240

[7] M. Naor and A. Shamir, “Visual cryptography,” Advances in Cryptology: Eurprocrypt'94, pp. 1-12, 1994.

[8] E. R. Verheul and H. C . A. v. Tilborg, “Constructions and properties of k-out-of-n visual secret sharing schemes,” Designs Codes Crypto., vol. 11, pp. 179-196, 1997.

[9] H. Koga, “A general formula of the (t,n)-threshold visual secret sharing scheme,” in Advances in Cryptology, Asiacrypt, pp. 328-345, 2002.

[10] Adhikari and S. Sikdar, “A new (2, n)-visual threshold scheme for color images,” in Proc. INDOCRYPT 2003, Berlin, pp. 148-161, 2003.

[11] Blundo, P. D'Arco, A.D. Santis, and D.R. Stinson, “Contrast optimal threshold visual cryptography schemes,”

[12] A.G.Bors and LPitas “Embedding parametric digital signatures in images” ***proc of*** *EUSIPCO*

[13] N.Nikolaidis and LPitas “Copyright protection of images using robust digital signatures” *proc.* ***Of*** *ICASSP-96,* Atlanta, USA, May 1996 (accepted).