IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 3, Ver. II (May – Jun. 2015), PP 79-85
www.iosrjournals.org

Copyright protection scheme based on visual Cryptography: A Review

Smriti sahu[1], Namita Tiwari[2]
[1](Computer Science, Maulana Azad National Institute of Technology, India)
[2](Ass. Professor, Department of Computer Science, Maulana Azad National Institute of Technology, India)

Abstract: *Management of digital images via internet and e-business has witnessed tremendous growth in last decades, resulting in vulnerability to copyright infringement, Manipulation and attacks. This paper reviews some of the current developments in the copyright protection techniques for digital images based on visual cryptography. The approaches reviewed in the paper are lined based on the false positive rate. This paper discusses the main approaches for copyright protection of digital images. This paper also discusses how those approaches can achieve the required security standard. The methods are measured against relevant performance metrics and set according to their respective environments and digital formats being used. Thus contributing sufficient knowledge so as to develop more secure scheme.*
Keywords: *Copyright Protection, Visual Cryptography.*

I. Introduction

Visual cryptography is a new cryptographic scheme pioneered by Moni Noar and Adi Shamir[1]. In this technique visual information (secret) is encrypted in such a way that decryption is done without any cryptographic computation. The visual cryptography technique encrypts a secret image into shadow images called shares. In the basic scheme secret image is encrypted into two shares such that both the shares can only recover the secret image, and either of the single share cannot leak any information about the secret. There are several generalizations of the basic scheme including k-out-of-n visual cryptography where in we have n shares and a minimum of k shares are needed to recover the secret. Characteristics of the scheme include 1. Perfect secrecy of secret messages. 2. Human Visual Systems (HVS) can decode the secret.

The basic code book of visual cryptography is shown in Fig 1 where each pixel is divided into 4 sub pixels. If a pixel p is white, one of the two columns tabulated under the white pixel in Fig 1 is selected. If p is black, one of the two columns tabulated under the black pixel is selected. If p is white, the superposition of the two shares always outputs two black and two white sub pixels, no matter which column of sub pixel pair is chosen during encoding. If p is black, it yields four black sub pixels.

Watermarking based on visual cryptography does not modify the pixels on the host image, balancing the characteristics like Imperceptibility, capacity, robustness, security, without any conflict. Hence termed as Lossless watermarking technique and is useful in protecting range of digital images.

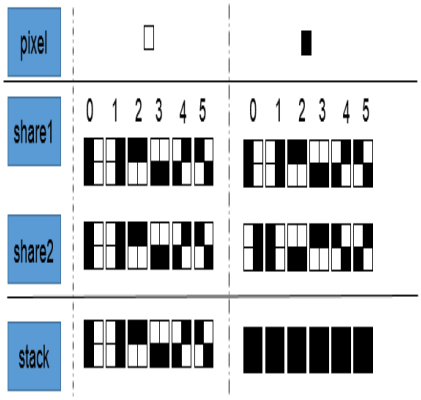


Fig. 1 Basic codebook

Steps involved in copyright protection based on visual cryptography are Owner Share Generation (OSG), Public share generation and Watermark Extraction (WE) as shown in Fig 2.Given a target image to be copyrighted and a secret key, a secret binary matrix, called master key is generated using some threshold technique. The bits of this master key and visual cryptography code table are then used to generate an owner share. The owner share is then registered with a certifying authority. Whenever there is a controversy regarding ownership identity, the other share called public share is computed from the controversial image using a similar process and the same secret key. But, to generate public share, the extraction algorithm does not require the original watermark. Both the shares are then combined using a combination function, to extract the watermark.

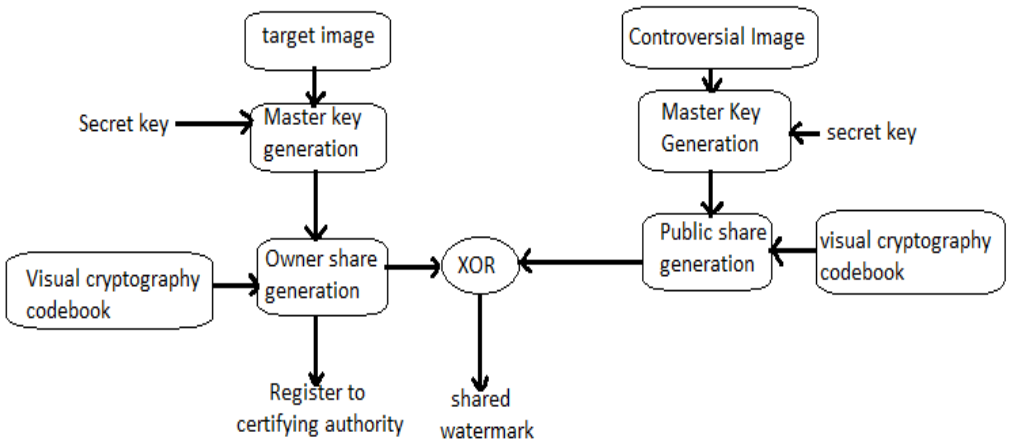


Fig. 2 Algorithm for copyright protection based on visual cryptography

Advantages of Watermarking based on visual cryptography over traditional watermarking scheme.
1. Original image is unaltered.
2. Visual cryptography based technique is lossless watermarking technique.
3. Constraint like embedding capacity is removed.
4. More secure

II. Existing approaches

(A)R. Hwang's method
In 2000 R. Hwang proposed Digital image copyright protection scheme based on visual Cryptography [2]. The proposed scheme used 2-2 visual cryptography to generate the verification information(Owner share).

Owner share generation Algorithm:
Input : host image M (K × 1 grey scale image), watermark image P (h×m).
Output: verification information.

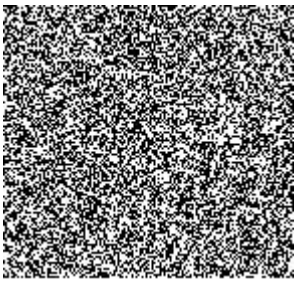
Step 1: Select a random number S as the secret key of the image M.S is known only to the owner.
Step 2: Use S as the seed to generate h×n different random numbers over the interval [0, k×l].
(We use Ri to denote the i-th random number.)
Step 3: Assign the i-th pair (v_{i1}, v_{i2}) of the verification information V based on Table 1.
Step 4: Assemble all the (v_{i1}, v_{i2}) pairs to construct the verification information V.
The verification information and the watermark image pattern is then registered to certifying authority.
If any issue regarding the image occurs then the owner provides the secret key to authority for verification.

Public share generation and watermark Extraction Algorithm:

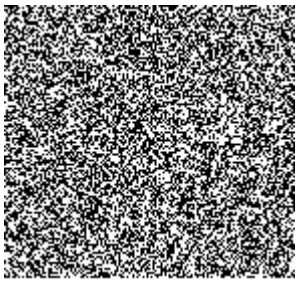
Step 1: Use S as the seed to generate h×n different random numbers over the interval [0, k×l].
(We use Ri to denote the i-th random number.)
Step 2: Assign the color of the i-th pixel of the watermark pattern P' based on Image M as follows:
2.1 Get the left-most bit, b, of the Ri-th pixel of Image F, and, if b is "1", then assign fi=(1, 0); otherwise, fi=(0,1).
2.2 If fi is equal to the i-th pair of V then assign the color of the i-th pixel of P' to be White; otherwise, assign it to be black.
Step 3: check If P' can be recognized as P through the human visual system. An example of the proposed scheme is shown in Fig 3.

(a)

(b)



(c)



(d)

(e)

Fig. 3 (a) host image (lena) (b) watermark image (c) Owner share (d) Public share (e) extracted watermark

(B)Ching-Sheng Hsu and Young-Chang Hou's Method

In 2005 C.S.Hsu and Y.C.Hou proposed Copyright protection scheme for digital images using visual cryptography and sampling methods [3] .The proposed method employed Sampling distribution of means to generate the master share .During sampling a private key is used which is kept secret. The proposed method enabled watermark image to be of any size regardless of the host image.

Owner share generation Algorithm:

Input: A gray-level host image H with M1×M2 pixels, a bi-level secret image S with N1×N2 pixels, and a private key K.

Output.: An ownership share O of size N1×N2 pixels.

Step 1: Compute the population mean μ of the pixel values of the host image H.

Step 2: Generate a list of random numbers L=(l1 , l2 , . . .), where l_m belongs to {1,2,…….$M_1 \times M_2$} by a random number generator seeded by K.

Step 3: Randomly select n(n≥30) pixel values $x_{t,1}, x_{t,2}, \ldots\ldots, x_{t,n}$. from the host image H (according to L) to form a sample mean $\dot{x}_t$

Step 4: For each pixel $s_{i,j}$ of the secret image S, determine the color of the pixel $o_{i,j}$ (with 4 sub pixels) in the ownership share OS according to the following encryption rules:

If $s_{i,j} = 0$ and $\bar{X}_t < \mu$ then $o_{i,j} =$  ,

else if $s_{i,j} = 1$ and $\bar{X}_t \geq \mu$ then $o_{i,j} =$, 

else if $s_{i,j} = 1$ and $\bar{X}_t < \mu$ then $o_{i,j} =$  ,

else $o_{i,j} =$  .

Step 5: Repeat steps 3 to 4 until all pixels of the secret image S are processed.

Public share generation and watermark Extraction Algorithm:

The public share construction and watermark extraction algorithm is similar to the owner share generation algorithm except step 4.In public share generation in step 4 For each pixel $o_{i,j}$ (with 4 sub pixels) of the ownership share OS, the color of the pixel $s_{i,j}$ in the secret image S' is determined according to the decryption rules which are similar to the encryption rules.

Table 1

The color of the *i*-th pixel in *watermark pattern* is	The left most bit of the *Ri*-th pixel of Image *M* is	Assign the *i*-th pair, (*vi*1, *vi*2), of *verification information V* to be
Black	"1"	(0, 1)
Black	"0"	(1, 0)
White	"1"	(1, 0)
White	"0"	(0, 1)

Table 2

Feature	mod(*k*, 3)	White		Stacked result	Black		Stacked result
		Share M	Share O		Share M	Share O	
$SV_k \geq T$	0						
	1						
	2						
$SV_k < T$	0						
	1						
	2						

Table 3

Rule	Comparison between $LL_1''(m,n)$ and μ_g	Identification Block ***m***
1	$LL_1''(m,n)<\mu_g$	
2	$LL_1''(m,n)\geq\mu_g$	

Table 4

Table 2

Rule	Comparison between $LL_1'(m,n)$ and μ_g	Watermark	Owner's Block ***o***
1	$LL_1'(m,n)<\mu_g$	0	
2	$LL_1'(m,n)<\mu_g$	1	
3	$LL_1'(m,n)\geq\mu_g$	0	
4	$LL_1'(m,n)\geq\mu_g$	1	

(C)M.S. Wang and W.C. Chen's Method

In 2007 M.S. Wang and W.C. Chen's Method proposed Digital image copyright protection scheme based on visual cryptography and singular value decomposition[4]. In this method singular value decomposition is used to generate the master share. The main property that the singular values (SVs) of an image do not change significantly when a small perturbation is added to an image is deployed in this scheme to attain robustness. This method results in pixel expansion that is the size o owner share is double than the size of watermark image.

Owner share generation Algorithm:

Input:A gray-level host image **H** of size M1×M2 pixels, a secret image **S** of size N1×N2 pixels, a window of size W×W pixels, a private key K, and a codebook C.

Output: An ownership share **O** of size 2N1×2N2 pixels.

Step 1: Select a list of pixel positions, P={p1 , p2 , . . . , pN1×N2}, by using a PRNG seeded with the private key K.

Step 2: Perform the SVD on the window centered at each pixel position in P and a sequence of SVs, $\Lambda=\lambda_1^1,\lambda_1^2\ldots\ldots\ldots\ldots,\lambda_1^{N_1\times N_2}$ consisting of the largest SV of each window, is acquired.

Step 3: Calculate the threshold T by using

$$T=\begin{cases}\lambda_1^{(N_1\times N_2+1)/2} & if\ N_1\times N_2\ is\ odd\\ \frac{1}{2}\left[\lambda_1^{(N_1\times N_2)/2}+\lambda_1^{1+\frac{N_1\times N_2}{2}}\right] & if\ N_1\times N_2\ is\ even\end{cases}$$

Step 4: Construct a master share **M** by utilizing the sequence ∧ and the threshold T according to the codebook In table 2.
Step 5: Create the ownership share **O** by mapping the master share **M** and the secret image **S** to the codebook.

Public share generation and watermark Extraction Algorithm:

Step 1-4 is exactly same as the owner share generation.
Step 5: Retrieve the secret image S' by stacking the master share M' and the ownership share **O**.
Step 6: Divide the retrieved secret image S' into nonoverlapping 2ẋ2 blocks, $S'_k(1 \le k \le N_1 \dot{x} N_2)$

Step 7: Perform the reduction process to obtain a reduced Secret image S'' by the following rules:

$$S'' = \begin{cases} 1, & if \ \sum_i \sum_j S'_k \ \geq 2 \\ 0, & if \ \sum_i \sum_j S'_k \ < 2 \end{cases}$$

(D)Young-Chang Hou and Pei-Hsiu Huang's Method

In 2011 Y.C.Hou and P.H.Huang proposed an image protection scheme based on visual cryptography and statistical property[3]. In this scheme comparison of two randomly selected pixel is done to generate the master share. This method allowed multiple watermarks to be registered for a single host image without causing any damage to other hidden watermarks. This method also allowed large watermark to casted for small host image.

Owner share generation Algorithm:
In owner share generation phase a secret key is used to generate random pixels for host image which is used for comparison. Following are the rules to generate the master share M:

Rule 1: If P(r_i) > P(r_{i+1}), then $m_{i,j}$ = □

Rule 2: If P(r_i) < P(r_{i+1}), then $m_{i,j}$= ■

Rule 3: If P(r_i)) = P(r_{i+1}), then we do the classification according to the median of the host image, that is,
If P(r_i)) > MD, then $m_{i,j}$= □
If P(r_i)) < MD, then $m_{i,j}$ = ■

Once we get the master share M, we can generate the ownership share O based on the encryption rules of visual cryptography and the contents of the master share M and the watermark W. Every pixel in O is generated as follows:
Rule 1: If $W_{i,j}$= 0 and $m_{i,j}$= □ then $O_{i,j}$= □
Rule 2: If $W_{i,j}$ = 0 and $m_{i,j}$= ■ then $O_{i,j}$= ■
Rule 3: If $W_{i,j}$= 1 and $m_{i,j}$= □ then $O_{i,j}$= ■
Rule 4: If $W_{i,j}$= 1 and $m_{i,j}$= ■ then $O_{i,j}$= □
Where P(r_i) is selected random pixel position, $m_{i,j}$ is a pixel of master share , $W_{i,j}$ is a pixel of watermark image and $O_{i,j}$ is a pixel of owner share. Obtained owner share is registered to the certifying authority.

Public share generation and watermark Extraction Algorithm:

Public share generation algorithm follows exactly the same algorithm as the owner share generation algorithm with the same secret key. The obtained public share is the superimposed with owner share to extract the watermark image.

(E)B.P.Devi, Kh. Manglem Singh and S.Roy's Method

In 2012 .P.Devi, Kh. Manglem Singh and S.roy proposed Dual Watermarking Scheme based on singular value decomposition and visual cryptography indiscrete wavelet transform. The proposed method is an improvement over the existing primary watermarking scheme based on singular value decomposition in the discrete wavelet transforms to improve the robustness.

Owner share generation Algorithm:

Input: Low frequency sub band $LL1'$of the image of size $N\times N$, binary watermark W of size $P\times Q$ and a key $K2$for generation of random location(m,n).

Output: An owner's share O of size $2P\times 2Q$

Step 1: Compute the global mean $\mu g$of the sub band $LL1'$.

Step 2: Generate a list of two-dimensional random number pair(m,n) over the interval 0,0 ,$(N-1,N-1)$ seeded by the key$K2$.

Step 3: For each pixel value in $LL1'$at the random location m, and the global mean μg from Column 2 in Table 4, and each watermark value $W\ i$, at location $(i,)$from Column 3 in Table 4, generate the owner's block **o** from Column 4 in Table 4.

Step 4: Repeat 3 until all pixels of the watermark W are processed.

Public share generation and watermark Extraction Algorithm:

Step 1-2 are as the owner share generation .

step 3: for each pixel value in $LL1''$ at the random location m,n and the global mean $\mu g'$ from Column 2 in Table3, and each sub-watermark value $W\ i,j$ at location $(i,j)$from Column 2 in Table 3, generate the master block m from Column 3 in Table 3.

Step 4: Repeat 3 until the end of all random locations generated by $K2$is exhausted.

(F)N.S.Gavini and S. Borra's method

In 2014 N.S.Gavini and S. Borra proposed a new visual cryptography based copyright protection scheme for high resolution images[7].This method deploys Central limit theorem on a correlation matrix obtained from the host image and block based visual cryptography.This method has 100% imperceptibility and has no limit on the size of watermark image and is robust.

Owner share generation Algorithm:

Input : secret key K ,watermark image c×d ,target image M×N.

Step 1: resize and remap the image T to obtain a modified image G of size MN/2^{α} and with 2^{β} colors.

Step 2: from image G obtain Correlation Matrix CM.

Step 3: Calculate mean μ of CM.

Step 4: obtain sample means μ_i, each of size n from CM Using secret key k as a seed.

Step 5: Obtain the elements of binary key matrix called master key (M) by Comparing each μ_i with the mean μ

Step 6: using the Block visual cryptography code table, Construct an owner share from the binary watermark and M .

The obtained owner share (OS) is then registered to a certifying authority.

Public share generation and watermark Extraction Algorithm:

Public share generation involves similar steps as the owner share Generation to obtain the public share (PS). The shared watermark is then extracted by performing OS XOR PS.

III. Performance parameters

Peak signal-to-noise ratio(PSNR) : PSNR is used to evaluate the image quality ie the similarity of original and attacked grey level image.

PSNR= $10 \times log_{10}\frac{255^2}{MSE}$

MSE=$\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(H_{i,j}-H_{i,j}^{'})^2$

Normalized Correlation (NC) : NC is used to evaluate the similarity of original and extracted image.

NC= $\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(B_{i,j}-B'_{i,j})}{M\times N}$

False Positive Rate (FPR) : FPR is a check of security. A false positive occurs if any wrong combination of owner and public share results in a trace of hidden watermark. Numerically if NC > 0.7 for wrong combination then false positive is said to be occurred.

FPR = $\frac{FP}{FP+TN}$, where FP= False positive and TN= True negative.

IV. Conclusion

In this paper lossless watermarking techniques for copyright protection based on visual cryptography are discussed. Table 6 shows the false positive rate of existing techniques. According to I.J.Cox [8] false positive rate of 10^{-6} can meet the security requirement. So there is still a good scope of improvement. Table 5 shows the robustness of existing techniques against variety of attacks for Lena image. It is also seen that the performance of the proposed technique depends on feature extracted from host image, visual cryptography code book used for share generation and retrieval method used to obtain the watermark. Other parameters on which further work can focus on are size of shares, capacity of watermark, complexity of scheme used and the format of images.

Table 5

Attacks	[5]		[3]		[6]		[4]		[7]	
	PSNR	NC	PSNR	NC	PSNR	NC	PSNR	NC	PSNR	NC
JPEG compression	23.34	0.96	39.54	0.98	32.04	0.99	32.55	0.99	-	0.96
Sharpening	19.98	0.95	29.15	0.94	23.79	0.79	19.09	0.97	-	0.90
Lightening	20.36	1.00	18.59	1.00	-	-	-	-	-	-
Darkening	20.74	0.99	18.59	1.00	-	-	-	-	-	-
Noising	18.30	0.92	24.47	0.89	15.58	0.90	18.83	0.99		0.90
Cropping	8.87	0.87	14.87	0.74	11.94	0.85	-	-	-	
Blurring	22.49	0.97	26.83	0.92	36.24	0.98	25.65	0.99	-	0.93
Geometric distortion	16.92	0.94	9.79	0.50	-	-	13.07	0.83	-	-
Rescaling	23.66	0.97	37.23	0.97	26.28	0.98	_	_	_	0.93
Jitter	12.11	0.88	19.08	0.80	_	_	-	-	_	_

Table 6

Method	False Positive Rate
R. Hwang 's[2]	0.1280
Y.C Hou and P.H. Huang's[5]	0.3899
C. S. Hsu and Y. C. Hou [3]	0.0070
K M singh's[6]	0.0150
M.S. Wang and W.C. Chen[4]	0.0058
N.S. Gavini and S.borra[7]	0.0030

References

[1]. M. Naor and A. Shamir, "Visual Cryptography", in Advances in Cryptology – Eurocrypt'94, Vol. 950 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1995, pp 1-12.

[2]. R. Hwang, "Digital image copyright protection scheme based on visual cryptography," Tamkang Journal of Science and Engineering, Vol.3, No.2, 2002, pp. 96-106.

[3]. C. S. Hsu and Y. C. Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods", Optical Engineering, Vol. 44, No. 7, 2005, pp. 1-10.

[4]. M.S. Wang and W.C. Chen, "Digital image copyright protection scheme based on visual cryptography and singular value decomposition", Opt. Eng., 46, Vol. 6, 2007, pp 1-8.

[5]. Y.C Hou and P.H. Huang, "Image Protection based on Visual Cryptography and Statistical Property", IEEE SSP, 2011, pp. 481-484.

[6]. B.P.Devi,K.M.Singh and S.Roy, "Dual image Watermarking Scheme based on Singular value decomposition and visual cryptography in discrete wavelet Transform ",International journal of computer application, vol. 50,No.12 , 2012.

[7]. N.S.Gavini and S. Borra, "Lossless Watermarking technique for copyright protection of high resolution images", IEEE Region 10 Symposium,2014,pp.73-78.

[8]. I.J. Cox, M.L. Miller and J.A. Bloom, "Watermarking applications and their properties", Proceedings of the International Conference on Information Technology: Coding and Computing- ITCC2000, 2000, pp.6–10