Contemporary Engineering Sciences, Vol. 8, 2015, no. 32, 1517 - 1528
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ces.2015.59277

A Watermarking Scheme for Digital Images Based on Visual Cryptography

B. Pushpa Devi[1], Kh. Manglem Singh[2,*], Sudipta Roy[3], Y. Jina Chanu[2] and T. Tuithung[4]

[1]Department of Electronics & Communication Engineering, NIT Meghalaya India

[2]Department of Computer Science & Engineering, NIT Manipur, Imphal, India
[*]Corresponding author

[3]Department of Computer Science & Engineering, Assam University, Silchar India

[4]Department of Computer Science & Engineering, NERIST, Itanagar, India

Abstract

A robust and blind watermarking scheme based on visual cryptography for copyright protection of digital images is proposed in this paper. It generates two shares of the secret image based on visual cryptography by comparing the pixel value of the image with the mean of the pixel values in each image block. The experimental results show that the proposed scheme clearly verifies the copyright of the digital images and is more robust in comparison with other visual cryptography based watermarking methods on a variety of attacks.

Keywords: Copyright protection, Visual cryptography, Share, Robust, Cat map

1 Introduction

Copyright protection of the digital multimedia contents that can be copied easily without loss of quality with no limitation on the number of copies, tempered and redistributed illegally without authorization is receiving attention [1]. A good solution to this problem is the digital watermarking, which embeds the copyright

information, known as the watermark to the original digital data to be protected without degrading it, but it can be detected or extracted later by the owner to prove his copyright in the case of legal dispute [2,3]. For copyright-related applications, the watermarked digital data is expected to be robust to various kinds of geometrical and removal attacks [4,5]. Some researchers propose detection based watermarking techniques such as one based on visual cryptography (VC) that does not alter the original image in order to preserve the visual quality of the image, but generates two shares known as the ownership share, which is registered to a certified authority (CA), used later for verification and identification share, which is generated from the suspected copyrighted document, to be used with the ownership share [6]. Possessing of either one of the shares can not reveal any information related to the copyright, but stacking of two shares, which are printed on the transparency sheets conveys the meaningful details about the copyright information.

Hwang proposed a robust and blind copyright protection scheme based on visual cryptography that uses the most significant bit (MSB) for comparison with the global mean of the intensity of the image in generation of the shares [7]. Hassan et al showed that MSB based VC method can not reveal the secret message if the histogram of the grey-level image is either left-skewed or right-skewed [8]. To overcome the drawback of false alarm, Hsu et al proposed a blind and robust watermarking scheme for copyright protection of the image in spatial domain using visual cryptography that generates the ownership share based on the pixel value of the binary secret message bit, global mean of the pixel values in the image and mean of the neighbouring pixel values of a randomly selected pixel in the image [6]. Singh proposed a robust and blind copyright protection scheme based on visual cryptography that generates shares of the secret image by comparing the pixel value with the mean pixel value in that block [9]. Lou et al proposed a robust and blind copyright protection scheme based on visual cryptography that generates shares from the product of the normal-distribution random bit and the difference between the low and middle level wavelet sub-bands [10, 11]. Rawat et al proposed a robust and blind watermarking scheme based on visual cryptography that generates shares using the dc coefficient of the discrete cosine transform (DCT) of the block of size 8×8 of the image by comparing the mean dc coefficients of blocks with every dc coefficient from each block [12]. Wang et al proposed a robust and blind watermarking scheme for copyright protection based on visual cryptography and singular values of singular value decomposition (SVD) of the image that generates shares by comparing the mean of the largest singular values from each block in the image with the largest singular value of each block [13]. The methods mentioned in [6, 7, 9, 10, 13] are robust to many attacks, but it is still possible to reveal the secret message using unauthorized images. Guo et al proposed a robust watermarking scheme that embeds the principal component of the watermark of the shuffled SVD (SSVD) of the watermark into the largest singular value of the image block of the host image, and the right orthogonal matrix is kept as the key for the extraction [14]. False alarm

of their method is less. It was reported that the visual quality of the reconstructed image using SSVD is better than one that uses SVD only.

Motivated by the above discussion, a robust and blind copyright protection algorithm based on VC is proposed that generates shares based on visual cryptography.

The rest of the paper is organized as follows. Section 2 on gives brief a preliminary description about cat map transform and visual cryptography. Section 3 is on the proposed method. Section 4 is on Experimental results, followed by conclusions in Section 5.

2 Preliminaries

This section gives a brief overview of cat map for image scrambling and visual cryptography.

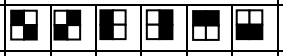
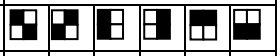
2.1 Cat Map

Arnold cat map transform is used as a scrambling method for the coordinates of the image, realizing the effect of image encryption [15]. For an image of size $N \times N$, the cap map is described by

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{1}$$

where (x, y) denotes the original pixel coordinates, (x', y') denotes the coordinates of pixel after applying cat map, a and b are the positive integers, and known as the control parameters, which along with the value of N decide the period P.

Table 1. A 2-out-of-2 VC

Pixel	White	Black
Share 1		
Share 2		
Stacked result		

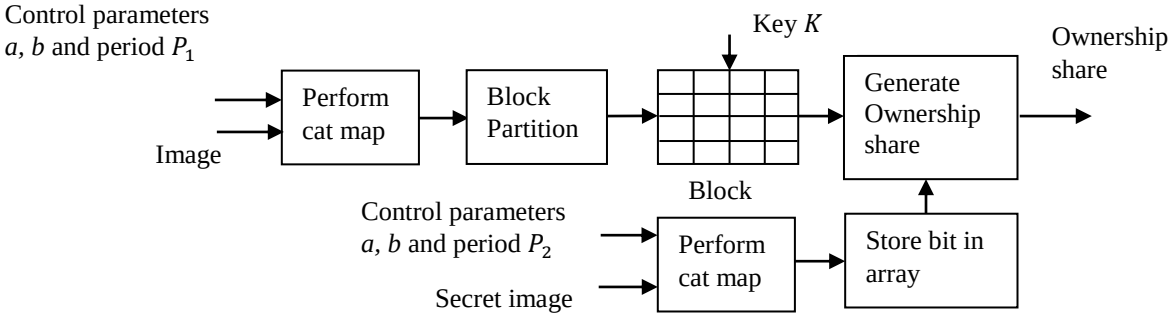


Figure 1. Schematic diagram of the proposed ownership share generation

2.2 Visual Cryptography

Naor and Shamir introduced visual cryptography in their seminal work in which a secret message is encrypted in a perfectly secure way in more than one shares such that the secret can be decrypted directly by the human visual system [16]. Table 1 illustrates how a binary image of size $M \times N$ is divided into two shares of size $2M \times 2N$ for a 2-out-of-VC, where each pixel of the secret image is expanded to 2×2 subpixels in the shares.

3 Proposed Technique

In this section, the proposed copyright protection scheme is proposed. The scheme is divided into two phases: ownership share construction and identification share construction. Cat map is applied to both the luminance channel of the image and binary secret image in ownership share generation to have the shuffled effect. The ownership share generation based on VC is as follows.

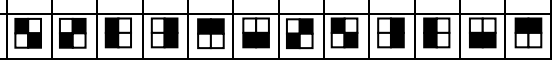
3.1 Ownership Share Generation Scheme

Let L be a luminance channel of host color image H of size $M_1 \times M_2$, W be the binary secret image of size $N \times N$, a and b be the control parameters of cat map for shuffling of pixel coordinates of luminance channel of the image and encrypting the secret image, P_1 and P_2 be the periods of cat map for the luminance channel of the image and the secret image respectively, K be a private key for selecting the block B_i, and C_1 be the codebook as shown in Table 2. Figure 1 shows the schematic diagram of the proposed ownership share generation scheme introduced as follows.

Table 2. Codebook C_1 for generation of ownership share

Feature	$B_i(3,3) < \mu_i$												$B_i(3,3) \geq \mu_i$											
scrambled bit	0						1						0						1					
$\text{mod}(i,6) =$	0	1	2	3	4	5	0	1	2	3	4	5	0	1	2	3	4	5	0	1	2	3	4	5
Ownership share																								

Table 3. Codebook C_2 for generation of identification share

Feature	$B_i'(3,3) < \mu_i'$						$B_i'(3,3) \geq \mu_i'$					
$\text{mod}(i,6) =$	0	1	2	3	4	5	0	1	2	3	4	5
Identification share												

O1. Perform conversion of the color host image H of size $M_1 \times M_2$ to obtain the luminance channel L. If the image is not square, padding is done using the nearest pixel values.

O2. Apply cat map on the secret image W of size $N \times N$, N_2 times using the control parameters a, b and period P_2 (where $N_2 < P_2$). Store the encrypted secret image bit in an array.
O3. Generate a list of random numbers $\{i \mid \text{such that total number of random numbers} = N \times N\}$ using pseudo random number generator (PRNG) with the private key K.
O4. Apply cat map on the luminance channel L, N_1 times using the control parameters a, b and period P_1 (where $N_1 < P_1$). Then divide the shuffled image into several blocks of size 5×5.
O5. Select a random block B_i, where i denotes the random block. $B_i(3,3)$ is the centre pixel value in the block. Find the mean value μ_i of all pixels in the block.
O6. Construct the ownership share block o_i based on the feature value ($B_i(3,3) < \mu_i$ or $B_i(3,3) \geq \mu_i$), scrambled secret image bit and $\mathrm{mod}(i, 6)$, as shown in the codebook C_1 of Table 2.
O7. Repeat Steps O5-O6 until all the secret image bits are exhausted. Finally, all the ownership share blocks are combined to form the ownership share O.

After the construction of the ownership share, the secret image, the private key K, the control parameters a, b and the periods P_1, P_2 must be kept secretly by the copyright owner, and the ownership share O should be registered to a CA for further authentication.

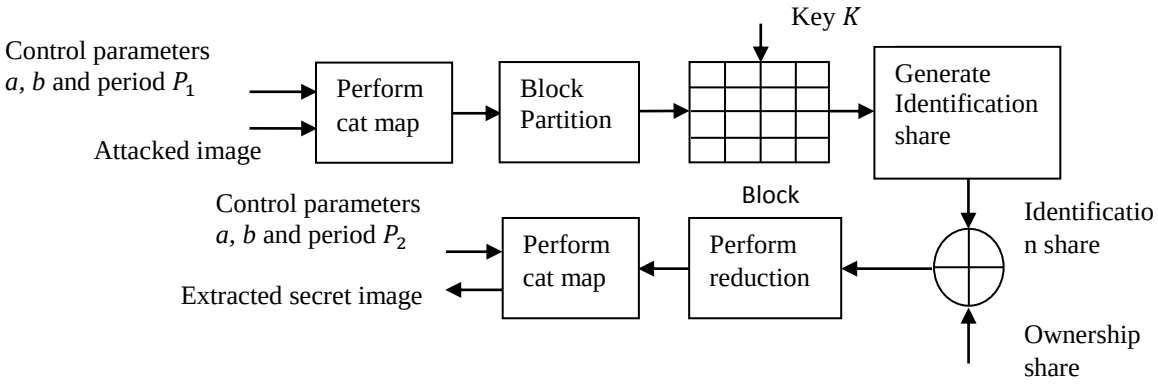


Figure 2. Schematic diagram of the proposed identification share generation and detection of secret message.

3.2 Identification Share Generation Scheme

Figure 2 shows the schematic diagram of the proposed identification share generation and secret image detection scheme. Some common geometric attacks and removal attacks may degrade the copyrighted image. Let H' be the probably attacked host color image of size $M_1 \times M_2$, L' be the luminance channel of the attacked image, a and b be the control parameters of cat map for shuffling of pixel coordinates of the image, P_1 be the period of cat map for the luminance channel, P_2 be the period of cat map for realizing decryption for the revealed secret image, K be the private key for selecting the block B_i', and C_2 be the codebook as shown in Table 3. The detection step can be formally defined as follows.

I1. Perform conversion of the attacked host color image $H^{'}$ of size $M_1 \times M_2$ to obtain the luminance channel $L^{'}$. If the image is not square, padding is done using the nearest pixel values.
I2. Generate a list of random numbers $\{i \mid such \ \ that \ total \ number \ of \ random \ numbers = N \times N\}$ using pseudo random number generator with the private key K.
I3. Apply cat map on the luminance channel $L^{'}$, N_1 times using the control parameters a, b and period P_1 (where $N_1 < P_1$). Then divide the shuffle image into several non-overlapping blocks of size 5×5.
I4. Select a random block $B_i^{'}$, where i denotes the random block. $B_i^{'}(3,3)$ is the centre pixel value in the block. Find the mean value $\mu_i^{'}$ of all pixels in the block.
I5. Construct the identification share block d_i based on the feature value ($B_i^{'}(3,3) < \mu_i^{'}$ or $B_i^{'}(3,3) \geq \mu_i^{'}$) and $\mathrm{mod}(i, 6)$, as shown in the codebook C_2 of Table 3.
I6. Repeat Steps I4-I5 until all the randomly selected block $B_i^{'}$ are exhausted. Finally, all the identification share blocks are combined to form the identification share D.
I7. Retrieve the secret image $W^{'}$ of size $2N \times 2N$ by stacking the ownership share O and the identification share D.
I8. Divide the retrieved secret image $W^{'}$ into non-overlapping 2×2 blocks $s_{j,k}^{'}$ $(1 \leq j, k \leq 2)$.
I9. Perform the reduction process to obtain a reduced secret image $W^{''}$ of size $N \times N$ by the following rules:

$$w = \begin{cases} 1, \text{if } \sum_j \sum_k s_{j,k}^{'} \geq 2 \\ 0, \text{if } \sum_j \sum_k s_{j,k}^{'} < 2 \end{cases} \quad (2)$$

where w is a binary pixel in $W^{''}$.
I10. Scramble the secret message $W^{''}$ by cat map $(P_2 - N_2)$ times using the control parameters a and b to obtain the descrambled secret message $W^{'''}$.

4. Experimental Results

A set of experiments was performed to verify the robustness of the proposed copyright protection algorithm using several images and a binary watermark. Representative images of size 512×512 and a binary watermark are shown in Figure 3. To evaluate the robustness of the proposed method, the proposed method was tested using ten different types of attacks: JPEG compression, rotation, median filtering, cropping, scaling, impulse noise, blurring, Gaussian noise, sharpening and Gamma correction. The normalized correlation (NC) is used to measure the similarity between the original secret image and the revealed secret image. It is defined as

$$NC = \frac{\sum_{m=1}^{N_1} \sum_{n=1}^{N_2} \overline{W(m,n) \oplus \widehat{W}(m,n)}}{N_1 \times N_2} \quad (3)$$

where $W(m,n)$ and $\widehat{W}(m,n)$ represent the original secret image and the detected secret image respectively, $\oplus$ denotes the exclusive-or (XOR) operation and $N_1 \times N_2$ is the size of the secret image.

(a) (b) (c) (d) (e) (f) (g) (h) (i) (j) (k)

Figure 3. Representative images: (a) Lena, (b) Mandrill, (c) Building, (d) Aptus, (e) Goldhill, (f) Zelda, (g) Airplane, (h) Barbara, (i) Tiffany, (j) Girl and (k) binary watermark

PSNR is used to measure the quality of the attacked image. It is given by

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \tag{4}$$

where MSE stands for mean squared error between the original image and the attacked image.

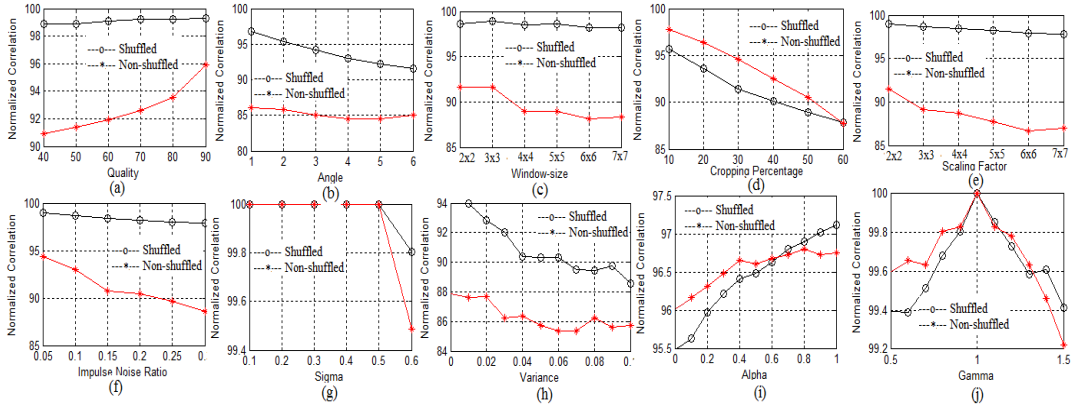


Figure 4. Comparison between shuffled and non-shuffled approaches : (a) JPEG compression, (b) Rotation, (c) Median filter, (d) Cropping, (e) Scaling, (f) Impulse noise, (g) Blurring, (h) Gaussian noise, (i) Sharpening and (j) Gamma correction attacks

Table 4. Robustness test for different methods

Attack		Lou	Wang	Rawat	Hwang	Hsu	Singh	Proposed
JPEG Compression	Q=40	92.5146	95.2441	95.1172	94.7583	98.6914	98.7842	98.8694
	Q=50	93.5645	95.6714	95.6470	94.8145	98.7891	98.8965	98.9061
	Q=60	94.3701	96.2476	96.0913	94.9316	98.9111	98.9355	98.9624
	Q=70	95.5542	96.7554	96.7334	95.0366	99.0015	99.1260	99.1820
	Q=80	96.7261	97.1655	97.2168	95.0781	99.1724	99.2383	99.2529
	Q=90	97.9614	98.0664	98.0347	95.1978	99.4018	99.4751	99.4956
Rotation	$A = 1^0$	80.4224	81.5796	81.3306	93.3350	94.4190	96.2524	96.8032
	$A = 2^0$	78.9258	76.7163	76.4502	92.9810	92.6294	94.9878	94.9850
	$A = 3^0$	78.8257	73.7964	73.4766	92.6416	91.6333	93.9575	93.9603

Table 4. (Continued): Robustness test for different methods

	$A = 4^0$	78.4766	71.8335	71.7261	92.2510	91.0132	93.1592	93.2026
	$A = 5^0$	78.5547	70.1489	70.1001	92.0874	90.5859	92.3828	92.4556
	$A = 6^0$	78.6157	68.9307	68.8843	91.8750	90.1660	91.5942	916038
Median filter	ws=2 ×	93.5010	92.0239	92.0435	94.4434	97.7539	98.4204	98.4666
	ws=3 ×	95.3345	93.9209	94.0088	94.6680	98.3667	98.7402	98.7523
	ws=4 ×	92.0313	90.5982	90.8691	94.3188	97.4683	98.0713	98.1070
	ws=5 ×	92.4536	91.2720	91.5576	94.3335	97.8198	98.1250	98.1371
	ws=6 ×	89.5947	89.2529	89.4409	94.2114	97.1777	97.7979	97.7979
	ws=7 ×	88.6523	89.9634	90.1953	94.2188	97.5196	97.8638	97.8831
Cropping	%C=10	97.5317	85.0415	81.9751	95.0488	88.3447	95.6616	95.9741
	%C=20	95.3052	78.3960	76.4014	94.8242	85.8008	92.4976	92.9199
	%C=30	93.4277	74.4287	74.4068	94.7046	83.9868	90.3833	90.6567
	%C=40	91.2598	75.3687	76.5112	94.2187	84.1919	88.8599	88.9844
	%C=50	89.1431	76.9287	79.1284	93.9087	89.9634	87.8150	87.9370
	%C=60	87.0312	74.0649	72.4512	93.4253	86.7505	86.8921	87.0801
Scaling	F=2 × 2	96.9727	93.5864	93.7085	94.4922	98.2837	98.5205	98.5862
	F=3 × 3	93.6597	91.6479	91.8994	94.3017	97.6441	98.0933	98.1614
	F=4 × 4	89.5996	90.3662	90.5737	94.1675	97.2558	97.7954	97.8879
	F=5 × 5	86.4062	89.3384	89.6314	94.0479	96.9702	97.5366	97.5804
	F=6 × 6	83.9038	88.5840	88.6548	93.9868	96.6748	97.3316	97.3825
	F=7 × 7	82.3389	87.8882	87.9467	93.9380	96.5234	97.1875	97.2165
Impulse Noise	R=.05	85.4639	80.1611	80.9058	94.8731	93.1763	98.6303	98.6885
	R=.10	83.5498	76.2768	76.7554	94.3140	91.2329	97.4316	97.4821
	R=.15	82.2339	74.4458	74.8682	93.8184	90.2344	96.2109	96.4834
	R=.20	81.9702	72.1606	73.4546	93.3301	89.3555	95.1709	95.1993
	R=.25	81.3086	71.3281	72.4072	92.6953	88.4985	94.1480	94.2132
	R=.30	81.1426	70.8472	70.9155	92.2241	88.3423	93.2861	93.2710
Blurring	ζ=0.1	100.0000	100.0000	100.0000	95.4248	100.0000	100.0000	100.0000
	ζ =0.2	100.0000	100.0000	100.0000	95.4248	100.0000	100.0000	100.0000
	ζ =0.3	100.0000	100.0000	100.0000	95.4248	100.0000	100.0000	100.0000
	ζ =0.4	100.0000	100.0000	100.0000	95.4248	100.0000	100.0000	100.0000
	ζ =0.5	100.0000	100.0000	100.0000	95.4248	100.0000	100.0000	100.0000
	ζ =0.6	99.4971	99.0918	99.1431	95.3174	99.7046	99.7510	99.7583
Gaussian noise	V=.01	85.9521	83.8574	83.7622	93.3301	94.4971	94.1968	94.1113
	V=.02	84.8755	80.5835	80.2734	92.4683	92.8784	92.6660	92.9834
	V=.03	83.6816	78.1616	78.2373	91.9214	91.8604	91.6504	91.7065
	V=.04	82.9468	76.6406	76.6211	91.4648	91.1231	91.0303	91.1304
	V=.05	82.7734	75.2588	75.7788	91.1841	90.5298	90.3198	90.6055
	V=.06	82.1680	74.7656	74.7778	90.8789	90.1709	90.3711	90.1684
	V=.07	82.0898	74.2090	74.5947	90.4175	89.7412	89.9292	89.8071
	V=.08	82.0288	73.7402	73.8135	90.3101	89.3848	89.6289	89.7559
	V=.09	81.8384	73.2788	73.0395	90.0366	89.2358	89.5679	89.4580
	V=.10	81.5845	73.0981	73.0713	89.8315	89.1626	89.3530	89.3384
Sharpening	α =.1	95.5420	87.4463	87.9419	93.4131	95.3540	96.3428	96.4941
	α =.2	95.7251	87.8857	88.3032	93.4888	95.5298	96.5137	96.6431
	α =.3	95.7520	88.2373	88.6914	93.5767	95.6592	96.6089	96.7700
	α =.4	95.8105	88.5034	88.9453	93.6426	95.8130	96.7188	96.9043
	α =.5	95.9473	88.7231	89.1553	93.7134	95.8814	96.8408	97.0020
	α =.6	96.1084	88.8159	89.2651	93.7427	95.9692	96.9165	97.0898
	α =.7	95.9668	89.0356	89.4751	93.7720	96.0693	97.0166	97.1338
	α =.8	96.0669	89.1699	89.5947	93.8135	96.1597	97.0752	97.1973
	α =.9	96.0449	89.2505	89.6899	93.8355	96.2280	97.1045	97.2339
	α =1	96.1865	89.3384	89.7437	93.8550	96.2720	97.1240	97.2900
Gamma correction	G=.6	98.7549	96.2476	97.0142	89.8462	98.9258	99.0088	99.0747
	G=.7	99.0747	97.1826	97.7710	91.2329	99.2187	99.2432	99.2969
	G=.8	99.2163	98.1787	98.5254	92.1973	99.5142	99.4507	99.5190
	G=.9	99.5361	99.1577	99.2407	94.4312	99.7559	99.7534	99.7168
	G=1	100.0000	100.0000	100.0000	95.4248	100.0000	100.0000	100.000
	G=1.1	99.5044	99.0601	99.2505	94.6265	99.6753	99.7412	99.7925
	G=1.2	99.3042	98.1909	98.6475	93.9356	99.4336	99.4995	99.5850
	G=1.3	99.0527	97.3022	97.9932	94.7070	99.1870	99.2627	99.3579
	G=1.4	98.9893	96.4990	97.3926	93.4570	98.9697	99.1040	99.1358
	G=1.5	98.7329	95.6714	96.7822	93.2007	98.7524	98.9380	98.9014

It was found experimentally that the proposed method with the block-size of 5×5 gives higher NCs on different attacks, however results were not shown due to the shortage of space.

Figure 4 shows comparison of the proposed method for selecting between shuffled and non-shuffled approaches for pixel coordinates on Lena image for various attacks. It was found that the proposed method gives better with the shuffling of the coordinates of the host image for all attacks except cropping and gamma correction attacks in term of NC. In further results, shuffling is employed.

The proposed method was compared with other popular methods in transform domain such as Lou et al method [9], Wang et al method [13] and Rawat et al method [12] and in spatial domain such as Hsu et al method [6], Hwang method [7], and Singh method [9] that use VC. Table 4 shows comparison of the proposed method with the other methods for various attacks. Average NC values for ten images are shown in the table. For JPEG compression, rotation, median filter, scaling, impulse noise, Gaussian noise, sharpening and gamma correction attacks, the proposed method gives superior performance in comparison with other six methods in term of NCs., Lou et al method gives the best results for cropping attack and all the seven methods give same performance for blurring attack.

Figure 5 shows detected secret image from the attacked image by JPEG compression attack for quality of 90, rotation attack for angle of 1^0, median filter attack for filtering window-size of 3×3, cropping attack for cropping percentage of 10, scaling attack for scaling factor of 2×2, impulse noise attack for impulse noise ratio of 0.05, blurring attack for sigma of 0.4, Gaussian noise attack for zero mean and variance of 0.01, sharpening attack for alpha of 0.1 and gamma correction attack for gamma of 0.8 on Lena image for different methods. NCs of the detected secret image with respect to the original secret image, and PSNRs of the attacked host image were shown in the figure. It shows that the detected image is the best for the proposed method for rotation, median filter, scaling, blurring, Gaussian noise, sharpening attacks as seen from the visual quality of the images and in term of NCs.

Attack		Lou	Wang	Rawat	Hwang	Hsu	Singh	Proposed
JPEG Compressio	Q=90	NC=97.6563 PSNR=39.48	NC=97.0947 PSNR=39.48	NC=97.7295 PSNR=39.48	NC=99.5117 PSNR=39.48	NC=99.4873 PSNR=39.48	NC=99.2432 PSNR=39.48	NC=99.2920 PSNR=39.48
Rotation	$A = 1^0$	NC=79.8584 PSNR=21.01	NC=85.0098 PSNR=21.01	NC=85.4980 PSNR=21.01	NC=96.6309 PSNR=21.01	NC=95.5078 PSNR=21.01	NC=96.2646 PSNR=21.01	NC=96.7773 PSNR=21.01
Median filter	ws = 3 × 3	NC=94.7266 PSNR=36.88	NC=94.9951 PSNR=36.88	NC=95.1416 PSNR=36.88	NC=98.9502 PSNR=36.88	NC=98.6816 PSNR=36.88	NC=98.5107 PSNR=36.88	NC=98.8770 PSNR=36.88

Cropping	C= 10%	NC=97.6074 PSNR=15.05	NC=85.2295 PSNR=15.05	NC=84.1797 PSNR=15.05	NC=84.9854 PSNR=15.05	NC=80.3467 PSNR=15.05	NC=95.1660 PSNR=15.05	NC=95.7275 PSNR=15.05
Scaling	F= 2 × 2	NC=96.9482 PSNR=32.99	NC=94.7998 PSNR=32.99	NC=95.0439 PSNR=32.99	NC=98.6328 PSNR=32.99	NC=98.7061 PSNR=32.99	NC=98.5107 PSNR=32.99	NC=98.9746 PSNR=32.99
Impulse noise	R=.0 5	NC=84.8389 PSNR=23.44	NC=80.3955 PSNR=23.34	NC=81.3477 PSNR=23.38	NC=99.2188 PSNR=23.41	NC=93.6768 PSNR=23.38	NC=98.7061 PSNR=23.43	NC=97.8027 PSNR=23.43
Blurring	ζ = 0.4	NC=99.4141 PSNR=51.71	NC=98.8281 PSNR=51.71	NC=99.1943 PSNR=51.71	NC=99.8291 PSNR=51.71	NC=99.8047 PSNR=51.71	NC=99.6582 PSNR=51.71	NC=99.8047 PSNR=51.71
Gaussian noise	V= 0.01	NC=85.2051 PSNR=24.77	NC=83.3496 PSNR=24.80	NC=83.4229 PSNR=24.77	NC=93.7500 PSNR=24.80	NC=94.1650 PSNR=24.77	NC=94.0186 PSNR=24.77	NC=94.5068 PSNR=24.77
Sharpening	α = 0.1	NC=94.3848 PSNR=24.56	NC=86.0596 PSNR=24.56	NC=86.8896 PSNR=24.56	NC=95.4590 PSNR=24.56	NC=94.7510 PSNR=24.56	NC=95.2881 PSNR=24.56	NC=95.6299 PSNR=24.56
Gamma correction	G7= 0.8	NC=99.4629 PSNR=27.08	NC=98.9258 PSNR=27.08	NC=99.2188 PSNR=27.08	NC=100 PSNR=27.08	NC=99.8047 PSNR=27.08	NC=99.7559 PSNR=27.08	NC=99.6826 PSNR=27.08

Figure 5. Detected secret messages

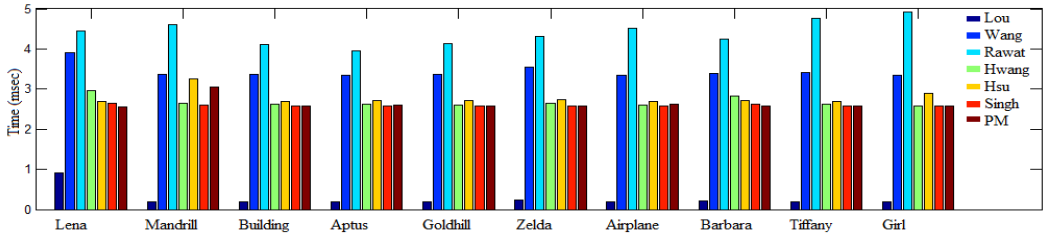


Figure 6. Comparison of computational time

False positive detection problem arises in most of VC-based algorithms including Lou et al, Wang et al, Hwang, Hsu et al and Singh methods. An unauthorized image can be used to extract or detect the secret image producing secret image, though the quality is not good. This means that anyone who can detect the secret image can claim ownership. Our method solves this false claim by encrypting the secret image prior to the ownership share generation, and it decrypts at the time of detection.

The computational time of the proposed method was compared with other methods as shown. in Figure 6. It is seen from the figure that the proposed scheme takes less time.

5. Conclusions

The paper describes a new watermarking algorithm based on visual cryptography for copyright protection of digital images. It generates two shares of the secret image based on visual cryptography by comparing the pixel value and the mean of pixel values in the image block of the shuffled image. The robustness of the proposed method was verified on different types of images for different attacks.

References

[1] J.C. Patra, J.E. Phua, and C. Bornand, A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression, *Elsevier Digital Signal Processing*, **20** (2010), no. 6, 1597-1611. http://dx.doi.org/10.1016/j.dsp.2010.03.010

[2] F. Petticolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Stefen Katzenbeisser, Artech House Inc, Boston, 1999.

[3] F. Hartung, and M. Kutter, Multimedia watermarking techniques, *Proc. IEEE*, **87** (1999), no. 7, 1079-1107. http://dx.doi.org/10.1109/5.771066

[4] J.J.K.Ò. Ruanaidh, and T. Pun, Rotation, scale and translation invariant spread spectrum digital image watermarking, *Elsevier Signal Processing*, **66** (1998), no. 3, 303-317. http://dx.doi.org/10.1016/s0165-1684(98)00012-7

[5] I.J. Cox, and M.L. Miller, The first 50 years electronic watermarking, *EURASIP Journal of Applied Signal Processing*, **2002** (2002), no. 2, 126-132. http://dx.doi.org/10.1155/s1110865702000525

[6] C.S. Hsu, and Y.C. Hou, Copyright protection scheme for digital images using visual cryptography and sampling methods, *Optical Engineering*, **44** (2005), no. 7, 077003-10. http://dx.doi.org/10.1117/1.1951647

[7] R.J. Hwang, A digital image copyright protection scheme based on visual cryptography, *Tamkang J. Sci. Engg*, **3** (2000), no. 2, 97-106.

[8] MA Hassan and MA Khalili, Self watermarking based on visual cryptography, *World Academy of Science, Engineering and Technology*, **8** (2005), 159-162.

[9] K.M. Singh, Dual watermarking scheme for copyright protection, *International Journal of Computer Science and Engineering Survey*, **3** (2009), 99-106.

[10] D.-C. Lou, H.-K. Tso, and J.-L. Liu, A copyright protection scheme for digital images using visual cryptography technique, *Elsevier Computer Standards & Interfaces*, **29** (2007), 125-131. http://dx.doi.org/10.1016/j.csi.2006.02.003

[11] T.-H. Chen, C.-C. Chang, C.-S. Wu, and D.-C. Lou, On the security of a copyright protection scheme based on visual cryptography, *Elsevier Computer Standards & interfaces*, **31** (2009), no. 1, 1-5.
http://dx.doi.org/10.1016/j.csi.2007.09.001

[12] S. Rawat, and B. Raman, A publicly verifiable lossless watermarking scheme for copyright protection and ownership assertion, *Elsevier AEU*, **66** (2012), no. 11, 955-962. http://dx.doi.org/10.1016/j.aeue.2012.04.004

[13] M.-S. Wang, and W.-C. Chen, Digital image copyright protection scheme based on visual cryptography and singular value decomposition, *Optical Engineering*, **46** (2007), no. 6, 067006-8. http://dx.doi.org/10.1117/1.2746906

[14] J.-M. Guo, and H. Prasetyo, False-positive-free SVD-based image watermarking, *Elsevier J. Vis. Commun. Image R.*, **25** (2014), no. 5, 1149-1163.
http://dx.doi.org/10.1016/j.jvcir.2014.03.012

[15] Y. Wang, K.-W. Wong, X. Liao, T. Xiang, and G. Chen, A chaos-based image encryption algorithm with variable control parameters, *Elsevier Chaos, Solitons and Fractals*, **41** (2009), no. 4, 1773-1783.
http://dx.doi.org/10.1016/j.chaos.2008.07.031

[16] M. Naor, and A. Shamir, Visual cryptography, Proc. Advances Cryptol. EUROCRYPT94, LNCS950, *Springer-Verlag*, Berlin, 1995, 1-12.
http://dx.doi.org/10.1007/bfb0053419

Received: October 11, 2015; Published: November 23, 2015