International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 10, Issue 2 [February. 2021] PP: 01-11

An application of visual cryptography scheme with digital watermarking in sharing secret information from car number plate digital images

Hana Stefanovic
Comtrade Information Technology School of Applied Studies
Belgrade, SERBIA
Ana Savic
School of Electrical and Computer Engineering of Applied Studies
Belgrade, SERBIA
Radosav Veselinovic
Faculty of Economics
Belgrade, SERBIA
Goran Bjelobaba
National Bank of Serbia
Belgrade, SERBIA
Corresponding Author: Hana Stefanovic, hana.stefanovic@its.edu.rs

ABSTRACT: *The paper form is a necessary condition for its publication, as well as its content. This paper presents an application of a visual cryptography scheme with a binary additive stream cipher which is used to form the meaningless shares (share images or multiple layers) of original digital image, hiding some secret information. Each share image holds some information, but at the receiver side only when all of them are superimposed, the secret information is revealed by human vision without any complex computation. Proposed algorithm for generating shares is applied in MATLAB programming environment, using MATLAB built-in functions to create sequences of pseudorandom numbers or streams, which are used to make share images of original digital image. The input digital image processing includes the image segmentation, plate localization for different orientations, resizing image and removing noise, is applied, while some edge detection algorithms and some morphological techniques are also used. The input image is then converted into a binary image, the share images are generated using pixel expansion scheme, and after that are sent to the receiver. At the received side, the shares could be printed in separate transparent sheets and overlapped in order to reveal the secret image, with some loss in contrast when compared to the original image. An algorithm is applied to car number plate digital images with watermark. Images are taken at the company parking place, while the company logo is used as a watermark. Digital image watermarking method is used to embed some data in a car number plate digital image in order to verify the credibility of the content or the identity of the owner. A simple C sharp Desktop application is also included, with test images taken for good and also imperfect detection conditions.*

Date of Submıssıon: 11-03-2021 Date of Acceptance: 26-03-2021

I. INTRODUCTION

A visual cryptography scheme is a technique for securely encrypting messages like pictures, text, etc., in such a way that the decryption can be performed by the human visual system, without any complex computation or aid of computers. The underlying cipher is essentially the one-time pad, so the system is unbreakable in the information theoretical sense. The original image is divided into meaningful or nonmeaningful shares, which are distributed among participants. During decryption, the original secret image is recovered through stacking all or some of the shares by the human visual system.

One of the best-known visual cryptography techniques has been credited to Moni Naor and Adi Shamir, developed in 1994. [1]. In their work, it is demonstrated that a visual secret sharing scheme can be used to broke up an original image into n shares, so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. Each share could be printed on a separate transparency, and decryption is performed by overlaying the shares. When all n shares were overlaid,

the original image would appear. There are several generalizations of the basic scheme including k-out-of-n visual cryptography [2] and using opaque sheets but illuminating them by multiple sets of identical illumination patterns under the recording of only one single-pixel detector. Some novel visual cryptography schemes combining visual cryptography with single-pixel imaging are also proposed [3], where the secret image is shared by multiple illumination pattern sequences and it can be recovered when the visual key patterns are projected onto identical items. There are also many different extended visual cryptography schemes [4], which encode a number of images in the way that when the images on transparencies are stacked together, the hidden message appears without a trace of original images. The decryption is also done directly by the human visual system with no special cryptographic calculations [5]. There are also many innovative ideas and extensions exist for the basic visual cryptographic model introduced till now. Random grid is a method to implement visual cryptography without pixel expansion [6]. The secret image is reconstructed with lower visual quality when applying random-grid-based visual cryptography, due to the fact that average light transmission of a share is fixed at 0.5 [7].

In this paper, transparencies are used to implement a one-time pad encryption, where one transparency is a shared random pad, and another transparency acts as the ciphertext. In algorithm implemented in this paper, an original image is split into two component images each having a pair of pixels for every pixel in the original image. These pixel pairs are shaded black or white according to the following rule: if the pixel in original image is black, the pixel pairs in the component images must be complementary; randomly shade one ■□, and the other □■. When these complementary pairs are overlapped, they will appear dark color. On the other hand, if the pixel in original image is white, the pixel pairs in the component images must match: both ■□ or both □■. When these matching pairs are overlapped, they will appear light gray. This pixel expanding scheme is used for sharing a car number plate digital images, while for customer pin code digital images we used 2 out of 2 visual cryptography model, where white pixel in shares is represented by both ▚ or both ▞. When these matching masks are overlapped, they will appear light gray. If the original pixel is black, it is represented by complementary masks: ▚ and ▞, or ▞ and ▚. When these complementary masks are overlapped, they will appear dark color, which is interpreted as black. In this model one transparency represents the ciphertext, while the other acts a secret key. There are many other expansion schemes specifying how to encode a single pixel, while some schemes are designed for color secret images [8].

Visual cryptography algorithms are used for watermarking [9], steganography, remote electronic voting [10], bank customer identification, anti-spam bot safeguard, massage concealment, key management, multi-layer ID cards, secured fingerprint or improving security of biometric authentication [11]. The concept of recursive hiding of secrets in visual cryptography [12] provides a method of hiding secrets recursively in the shares of threshold schemes, which permits an efficient utilization of the data, with many possible uses for authentication. In this paper, digital watermarking is also applied, in order to verify the credibility of the content or to recognize the identity of the digital content's owner. A visible digital watermarking technique is used, which means that the visible data is embedded as the watermark [13]. This is usually a logo or a text that denotes a digital medium's owner. In this paper a ITS (Comtrade Information Technology School) logo is used and applied into car number plate digital images taken at the company parking areas.

After isolating the plate on the input image and after its conversion from RGB layers to gray-scale layer, the contrast and brightness of the image are adjusted. A Median filter is used to reduce the noise from image, while Sobel edge detector is applied in order to increase the difference between the letters and the plate backing [14]. Visual Studio and C# to are used to create Windows Forms application given in this paper.

II. ALGORITHM OBJECTIVES AND SOME EXPERIMENTAL RESULTS

An original image captured using standard smartphone camera is presented in Fig. 1. A 41.3 MP image sensor with Carl Zeiss optics and Xenon flash (Nokia Lumia 1020) is used for all test images used for this research, while using the professional cameras, specifically designed for the task could generate high quality pictures, and could give better results [15].

Results after applying Median filter in order to remove a noise and Sobel detector [14] in order to increase the difference between the letters and the plate backing are given in Fig. 2 and Fig. 3.

Median filtering is a nonlinear operation often used in image processing to reduce noise and it is more effective than convolution when the goal is to simultaneously reduce noise and preserve edges [16]. An object can be easily detected in the image if the object has sufficient contrast from the background, as it is illustrated in Fig. 2.

Fig. 1 The original image

Fig. 2 The result image after removing noise using Median filter

Fig. 3 The result image after detecting edges using Sobel operator

Sobel detection is an image processing technique for finding the boundaries of objects within images, based on detecting discontinuities in brightness [14]. It is realized using MATLAB edge function and the result is given in Fig. 3. The binary gradient mask shows lines of high contrast in the image.

The secret image is then split into two share images, or shares, each having a pair of pixels for every pixel in the original image. These pixel pairs are shaded black or white according to the following rule: if the pixel in original image is black, the pixel pairs in the component images must be complementary; randomly shade one ■□, and the other □■. When these complementary pairs are overlapped, they will appear dark color. On the other hand, if the pixel in original image is white, the pixel pairs in the component images must match: both ■□ or both □■. When these matching pairs are overlapped, they will appear light gray. Boolean operation "XOR" is implemented by means of a visual "OR".

The shares generated according to this rule, are presented in Fig. 4, and Fig. 5, respectively. After superimposing two component images, the secret image will appear, but with some loss in contrast, as it is shown in Fig. 6.

It can be concluded that the decoded image is identified, although some contrast loss is observed. After superimposing two shares presented in Fig. 4. and Fig. 5, the secret image is decoded with 50% loss of contrast. Reconstructed pixel, consisting of two sub pixels, has a gray level of 0.5 if the original pixel is white, and gray level of 1 (black), if the original pixel is black, due to previously described rule. This is a reason of a 50% loss of contrast in the reconstructed image, but it is still visible.

It can also be concluded that due to pixel expansion, the width of the decoded image is twice as that of the original image. Some mathematical optimization models in order to maximize the contrast of recovered images are also proposed [17].

Proposed algorithm gives good results also for imperfect detection conditions, such as such as time of day, weather and angles between the cameras and the license plates [18], as it is presented in Fig. 7. Share images are shown in Fig. 8 and Fig. 9, while the reconstructed image is given in Fig. 10, including some additional filtering and image processing techniques before generating share images [19].

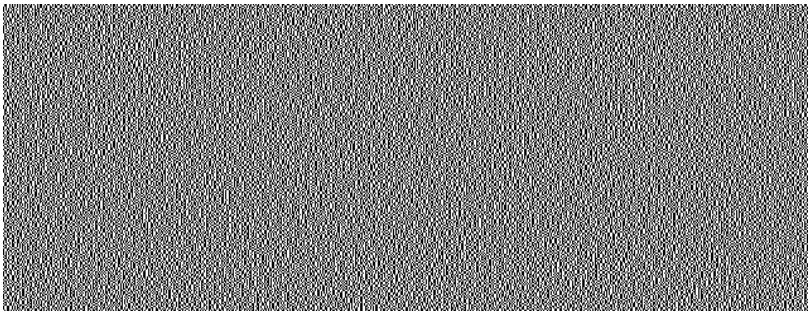

Fig. 4 Share image 1

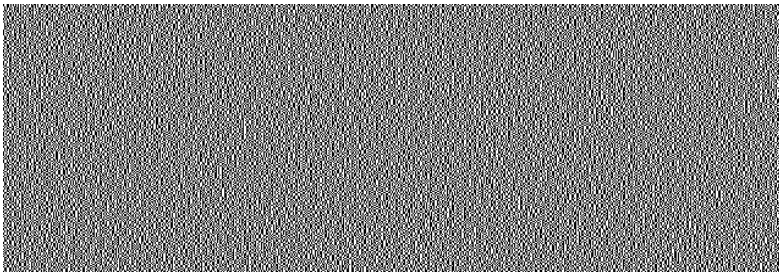

Fig. 5 Share image 2

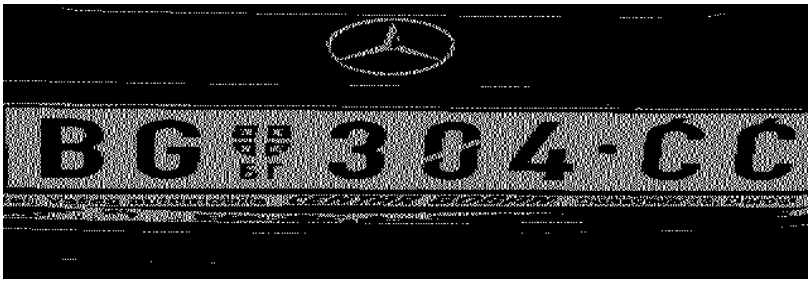

Fig. 6 The superimposed image

Fig. 7 The original image for imperfect detection conditions

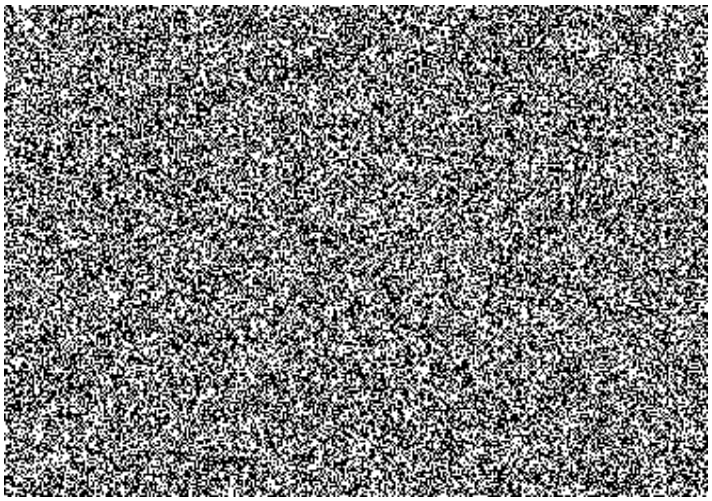

Fig. 8 Share image 1

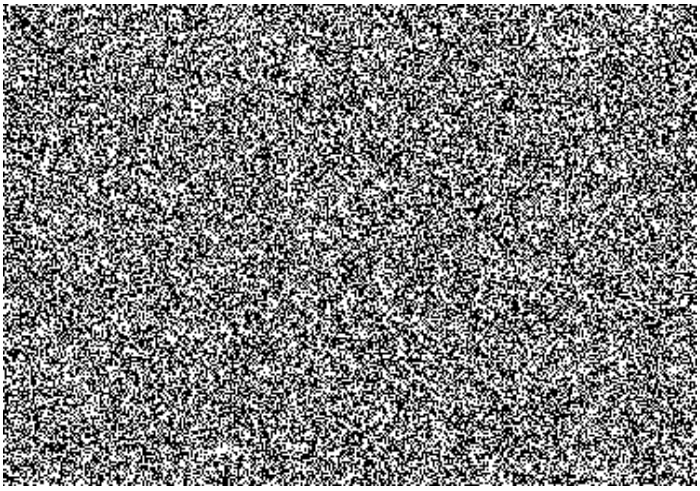

Fig. 9 Share image 2

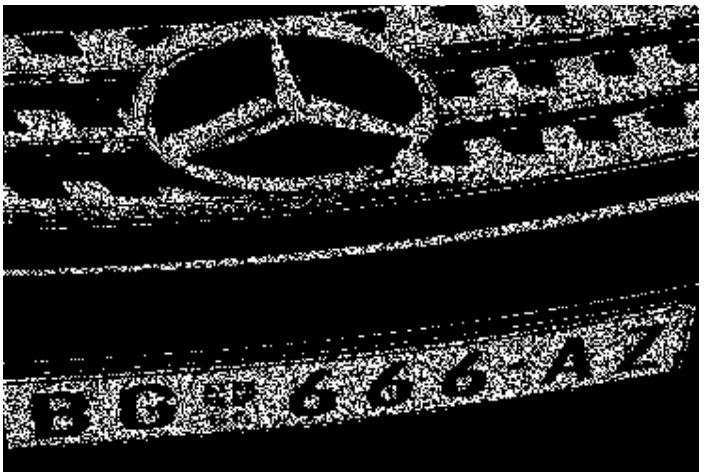

Fig. 10 The superimposed image

Digital watermarking provides an additional protection [20], as it is illustrated in Fig. 11. The ITS logo is used as watermark image, while the superimposed image, generated from share images, shows the recognized logo. Share images are shown in Fig. 12 and Fig. 13, while the recognized logo is given in Fig. 14.

Fig. 11 The original image with watermark

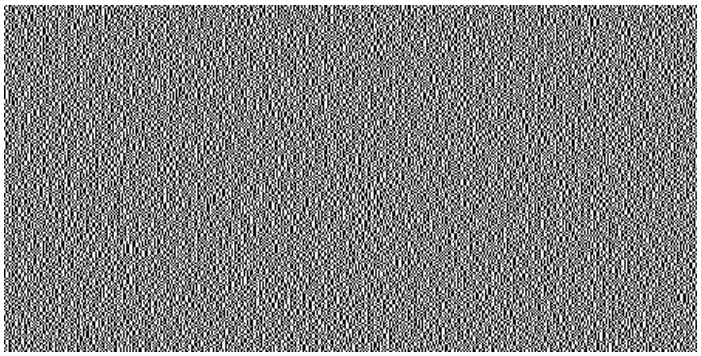

Fig. 12 Share image 1

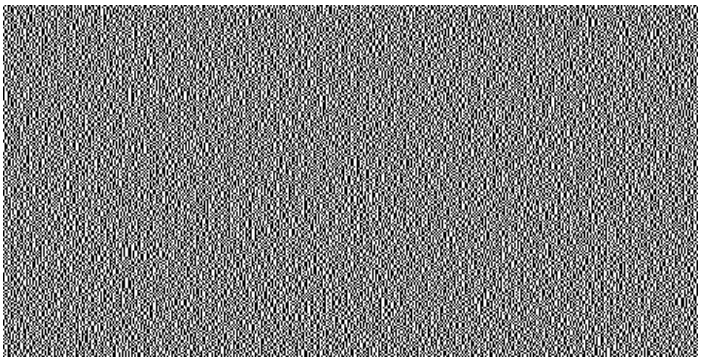

Fig. 13 Share image 2

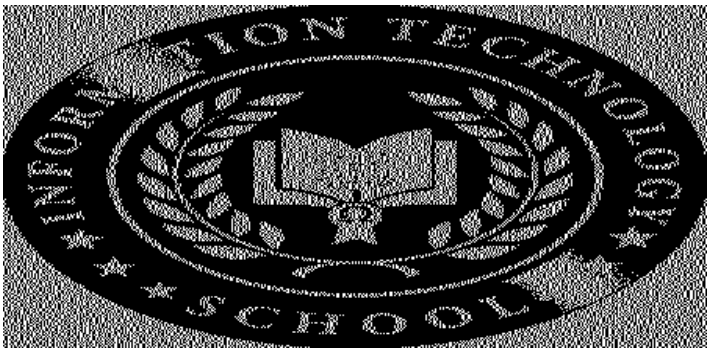

Fig. 14 The superimposed image

III. C# DESKTOP APPLICATION TEST RESULTS

Some results on test images given in Fig. 15, Fig. 17 and Fig. 19, using C# Windows Form Application are presented in Fig. 16, Fig. 18 and Fig. 20, without pixel expansion [21].

.

Fig. 15 Test1 image

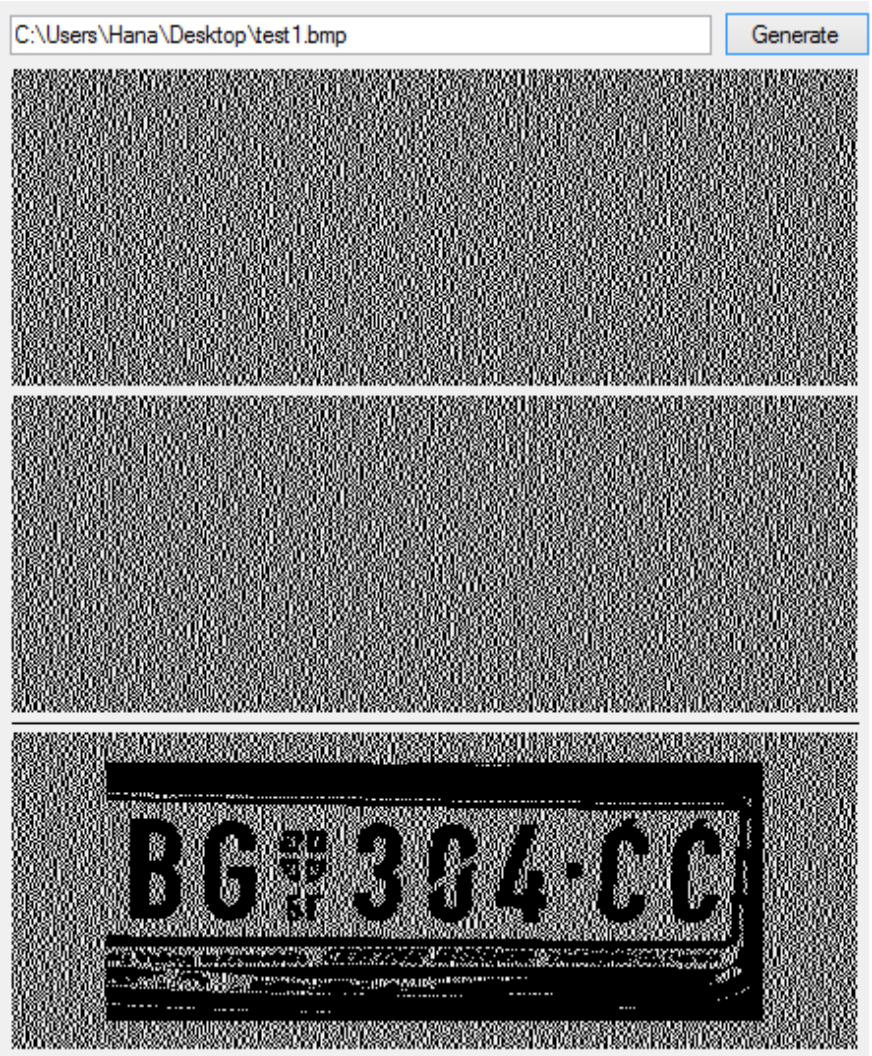

Fig. 16 Share images and the superimposed image for test1 image

Fig. 17 Test2 image

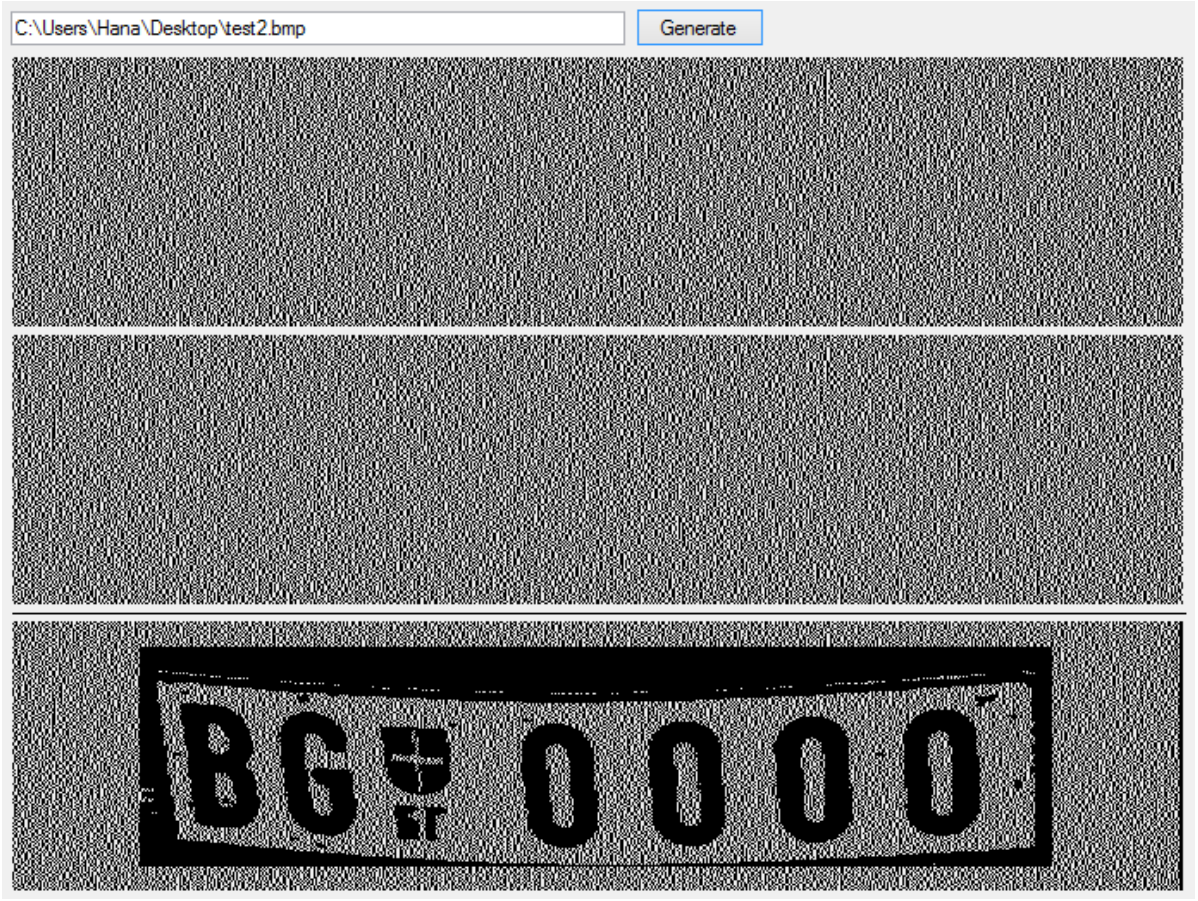

Fig. 18 Share images and the superimposed image for test2 image

Fig. 19 Test3 image

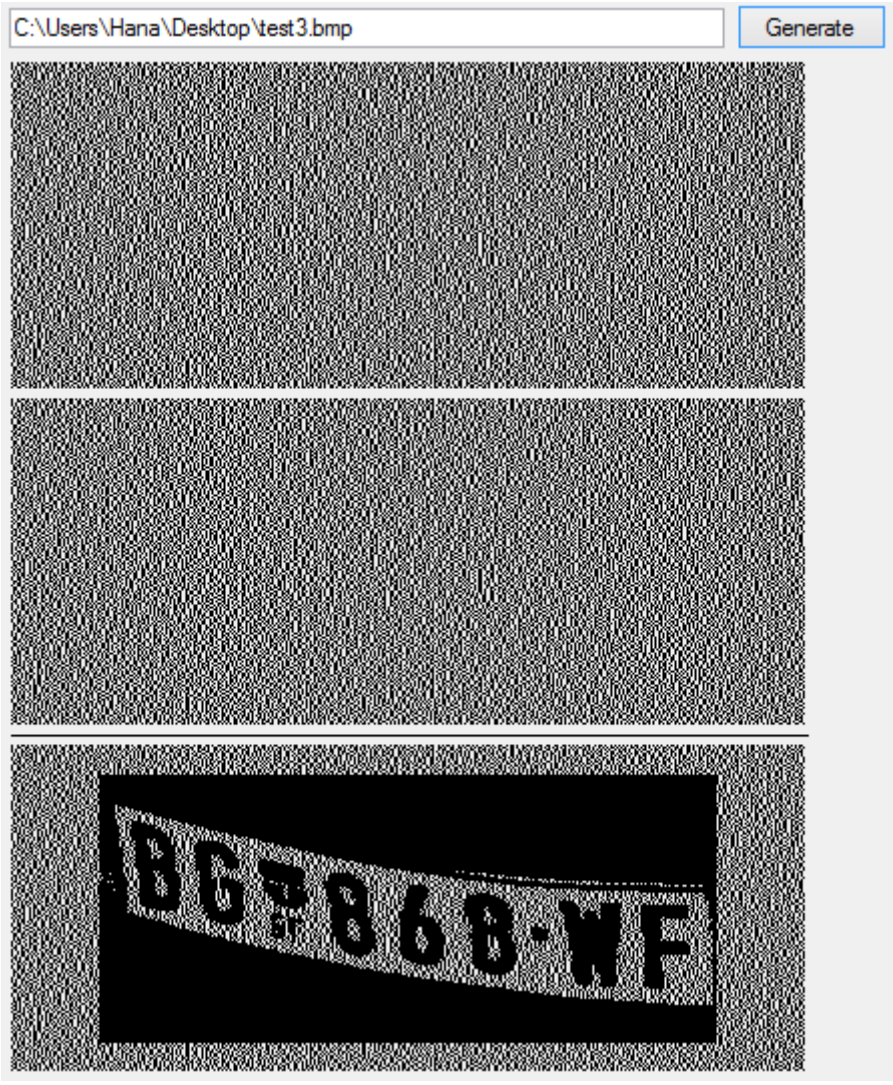

Fig. 20 Share images and the superimposed image for test3 image

IV. MATHEMATICAL BACKGROUND AND SECURITY OF VISUAL CRYPTOGRAPHY SHARING SCHEME

The structure obtained from either white or black pixel representation can be described by an $n * m$ Boolean matrix S_p where $p \in \{S_{white}, S_{black}\}$. Any given element s_{ij} of the matrix S is considered to be 1 iff the jth subpixel in the ith transparency is black. When the n transparencies are properly aligned, the resulting black subpixels are the Boolean OR of the columns for each row $i_1, i_2, \ldots, i_n$ of matrix S. Shares #1 and #2 would represent i_1 and i_2 respectively. Therefore, the following 2 * 4 Boolean matrices would be derived.

$$S_{white} = \{\{1,0,0,1\},\{1,0,0,1\}\} \quad (1)$$

$$S_{black} = \{\{1,0,0,1\},\{0,1,1,0\}\} \quad (2)$$

The matrix elements represent share assignments for share #1 and share #2 respectively. Since m subpixels constitute one original pixel and the overall visual effect of a black subpixel in any one of the shares causes that particular subpixel when combined to become black, inspection of the grey level is the method of determining the original colour of a pixel. The grey level of the combined share's subpixels is proportional to the Hamming weight $H(V)$ of the ORed m-vector V. The combined subpixels are interpreted by the human visual system as a black pixel if $H(V) > d$ and as a white pixel if $H(V) < d - \alpha m$ for some fixed threshold $1< d < m$ and relative difference $\alpha \rightarrow 0$. The use of threshold d and relative difference α is necessary in order to distinguish between the colors [8].

A case where visual cryptography is applied to the K out of N problem could begin with a person generating N shares from an original secret image. These N shares could be distributed via some communication channel, to N different participants with no prior knowledge of their particular share. In order to retrieve the original image, K out of the N participants would have to collaborate and overlay their shares. Any K out of N participants collaborating could reveal the original secret message, but fewer than K participants could reveal no information at all [2].

A solution to the K of N visual cryptography scheme can be described using two sets of $n * m$ Boolean matrices represented by B_0 and B_1. Each row in each matrix in B_0 or B_1 defines the values of m subpixels in corresponding shares. One of the matrices in B_0 is randomly chosen to share a white pixel, and to share a black pixel dealer randomly chooses one of the matrices in B_1. Chosen B_0 and B_1 sets are considered valid for the following conditions:

1. For any S in B_0, the "OR"ed V of any k of n rows satisfies $H(V) < d - \alpha m$
2. For any S in B_1, the "OR"ed V of any k of n rows satisfies $H(V) \geq d$
3. For any subset $\{i_1, i_2, \ldots, i_q\}$of $\{1, 2, \ldots, n\}$ with $q<k$, two sets of $q * m$ matrices obtained by restricting each $n * m$ matrix in B_0 and B_1, to rows $i_1, i_2, \ldots, i_q$ are not indistinguishable in the sense that they contain the same matrices with the same frequencies.

The first two conditions are referred to as contrast, while the third condition is referred to as security. In 2 by 2 scheme and four subpixels, we used different matrices:

$$S_{white} = \left\{\begin{bmatrix}0101\\0101\end{bmatrix}\begin{bmatrix}1010\\1010\end{bmatrix}\begin{bmatrix}0011\\0011\end{bmatrix}\begin{bmatrix}1100\\1100\end{bmatrix}\begin{bmatrix}0110\\0110\end{bmatrix}\begin{bmatrix}1001\\1001\end{bmatrix}\right\} \quad (3)$$

$$S_{black} = \left\{\begin{bmatrix}0101\\1010\end{bmatrix}\begin{bmatrix}1010\\0101\end{bmatrix}\begin{bmatrix}0011\\1100\end{bmatrix}\begin{bmatrix}1100\\0011\end{bmatrix}\begin{bmatrix}0110\\1001\end{bmatrix}\begin{bmatrix}1001\\0110\end{bmatrix}\right\} \quad (4)$$

The security of the visual secret sharing schemes depends up on the column permutation of the base matrices. The shares may reveal the information of the original image if less number of column permutations is taken for the encryption of the image. Both row and column-wise pixel expansion need to be done. If only the row-wise pixel expansion is done, the decrypted output looks like the stretched one which reduces the quality of the original image.

V. CONCLUSION

This paper contains description and demonstration of simple MATLAB-based visual cryptography scheme, where no decryption knowledge is required at the receiver side. The chipper could be send through e-mail, fax or via social networks, while only human visual system is needed to decode the secret image. One of disadvantages is loss in contrast in the reconstructed image, and also the fact that the perfect alignment of the transparencies is needed. The original formulation of described algorithm is restricted only to binary images, so some additional image processing techniques for color images are also applied. Digital watermarking is used in order to provide an additional protection. In future work, some techniques for improving the display quality of recovered images, and for maximizing the contrast of recovered images that are subject to density-balance and blackness constraints, would be applied.

REFRENCES

[1]. Naor, M., and Shamir, A. [1994] "Visual cryptography" Proc. Advances in Cryptology (Eurocrypt'94), pp.1-12.

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

[3]. Shuming, J., Feng, J., Yang, G., Ting, L., and Xiaocong, Y. [2020] "Visual cryptography in single-pixel imaging" Optics Express, Vol. 28: pp.7301-7313.

[4]. Ateniese, G., Blundo, C., Santis, A. De., and Stinson, D. R. [2001] "Extended capabilities for visual cryptography" Theoretical Computer Science, Vol. 250, Issue 1–2: pp.143-161.

[5]. Yan, J. W. [2010] "A comprehensive study of visual cryptography" Trans. Data Hiding and Multimedia Security V, pp. 70-105.

[6]. Wu, X. T., and Sun, W. [2013] "Generalized random grid and its applications in visual cryptography" IEEE Trans. Information Forensics and Security, Vol. 8, No. 9: pp.1541-1553.

[7]. Hou, Y. C., Wei, S. C., and Lin, C. Y. [2014] "Random-grid-based visual cryptography schemes" IEEE Trans. Circuits and Systems for Video Technology, Vol. 24, No. 5: pp.733-744.

[8]. Kang, I., Arce, G., and Lee, H. [2011] "Color extended visual cryptography using error diffusion" IEEE Trans. Image Process., Vol. 20, No. 1: pp.132-145.

[9]. Stinson, D. [1995] Cryptography Theory and Practice, CRC Press.

[10]. Wolchok, S., Wustrow, E., Isabel D., and Halderman, J. A. [2012] "Attacking the Washington, D.C., Internet Voting System" Conf. on Financial Cryptography & Data Security, pp.1-18.

[11]. Askari, N., Moloney, C., and Heys, H. M. [2015] "Application of visual cryptography to biometric authentication" Newfoundland Electrical and Computer Engineering Conf. (NECEC-2011), Retrieved 12 February 2015.

[12]. Gnanaguruparan, M., and. Kak, S. [2002] "Recursive Hiding of Secrets in Visual Cryptography" Cryptologia, Vol. 26: pp.68-76.

[13]. Priya, L. C. V., and Raj, N. R. [2017] "Digital watermarking scheme for image authentication" Int. Conf. on Communication and Signal Processing (ICCSP-2017), pp.2026-2030.

[14]. Gonzalez, R. C., Woods, R. E., and Eddins, S. L. [2009] Digital Image Processing Using MATLAB, Knoxville, TN:Gatesmark Pub.

[15]. Popovic, M. [2006] Digitalna obrada slike, Belgrade:Akademska misao.

[16]. Chong, J., Tianhua, C., and Linhao, J. [2013] "License Plate Recognition Based on Edge Detection Algorithm" Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing, pp.395-398.

[17]. Chiu, P., and Lee, K. [2011] "A Simulated Annealing Algorithm for General Threshold Visual Cryptography Schemes" IEEE Trans. Information Forensics and Security, Vol. 6, No. 3: pp.992-1001.

[18]. Pratt, W. K. [2007] Digital Image Processing, Inc. New York, NY, USA., John Wiley & Sons.

[19]. Stefanovic, H., Veselinovic, R., Bjelobaba, G., and Savic, A. [2017] "Optimizacija algoritmskih resenja za izdvajanje obelezja registarskih tablica u uslovima otezane detekcije" Info M 64/2017, pp.33-37.

[20]. Cox, I., Miller, M., Bloom, J., Fridrich, J., and Kalker, T. [2013] Digital Watermarking and Steganography, 2nd Ed., Elsevier.

[21]. Askari, N., Heys, H. M., and Moloney, C. M. [2013] "An Extended Visual Cryptography Scheme Without Pixel Expansion for Halftone Images" Proc. of IEEE Canadian Conf. on Electrical and Computer Engineering (CCECE 2013), Regina, Canada.