# An Investigation of Visual Cryptography and its Applications in Secure Communications

Elham Shahab
Dept. Computer Science
Islamic Azad University
dr.elhamshahab@gmail.com

Hadi Abdolrahimpour
Dept. Bio Mechanic
Islamic Azad University
Abdolrahimpour@yandex.com

***Abstract*—Secret sharing approach and in particular Visual Cryptography (VC) try to address the security issues in dealing with images. In fact, VC is a powerful technique that combines the notions of perfect ciphers and secret sharing in cryptography. VC takes an image (secret) as an input and encrypts (divide) into two or more pieces (shares) that each of them can not reveal any information about the main input. The decryption way in this scenario is done through superimposing shares on top of each other to receive the input image. No computer participation is required, thus showing one of the distinguishing features of VC. It is claimed that VC is a unique technique in the sense that the encrypted message can be decrypted directly by the human visual system.**

***Index Terms*— Visual cryptography, secret sharing, image encryption.**

## I. Introduction

With the increase in digital data and due to the recent development of computers and computer networks, the need for methods to protect digital information is becoming more necessary. Digital data can easily be transmitted or stored and during that process it may vulnerable to be eavesdropped or substituted by enemies if the data are not enciphered by some cryptographic algorithms.

In 1970's two important secure approaches were developed to deal with digital data while transmitting. They are the public key cryptosystem, which was proposed by Diffe-Hellman in 1976 [4], and the Data Encryption Standard (DES), which is a secret key cryptosystem adopted by the National Bureau of Standards in U.S.A. in 1977[4].

In the case of secure data storage, we have the same problems such as eavesdropping and substituting, and those threats can be taken care of through cryptographic technologies. However, we may have other threats such as troubles of storage devices or attacks of destruction. In order to tackle those attacks, one approach would be having as many copies of the secret as possible[2]. But, if we have many copies of the secret, the secret tends to leak out, and hence, the number of the copies should be as small as possible[2]. This contradictive requirement can be addressed by a Secret Sharing scheme (SS) technique , which was proposed by Adi Shamir in 1979[2]. Shamir published an article titled "How to share a secret" [3]. In this article, the following example was proposed to define a typical secret sharing problem:

"Eleven scientists are working on a secret project. They wish to lock up the documents in a cabinet so that the cabinet can be opened if and only if six or more of the scientists are present. What is the smallest number of locks needed? What is the smallest number of keys to the locks each scientist must carry?

The minimal solution uses 462 locks and 252 keys per scientist."

In the paper, (k, n)-threshold scheme was introduced by Shamir to generalize the mentioned problem and formulate it[2]. It can be explained as follows: Let S be the secret to be shared among n parties. A (k, n)-threshold scheme is a way to divide S into n pieces $S_1, S_2, \ldots, S_n$ that satisfies the conditions:

1. Knowledge of any k or more $S_i$ pieces makes S easily computable.
2. Knowledge of any $k-1$ or fewer $S_i$ pieces leaves S completely undetermined (in the sense that all its possible values are equally likely).

Secret Sharing scheme can be applied in different domains. One of the areas that are heavily used this approach is in Visual Secret Sharing (VSS). VSS is a powerful technique that combine the notion of perfect ciphering and Secret Sharing approach. This method uses the idea of hiding secrets within images. These images are encoded into multiple shares and later decoded without any computation. In fact, Visual Secret Sharing approach uses the characteristics of human vision to decrypt encrypted images. The decoding process is as simple as superimposing transparencies, which allows the main secret to be recovered. It would be a great advantage for this method that anyone can physically manipulate the elements of the system, and visually see the decryption process in action without any knowledge of cryptography and without performing any cryptographic computations.

## II. (K,N)-THRESHOLD SS SCHEME

(k, n)-threshold SS scheme illustrated in Figure 1. It shows that any k out of n shares can decrypt secret S but any k-1 or less shares do not leak out any information of S. Therefore, even if n-k shares are destroyed by an attacker, we are able to recover S from the remaining k shares[2]. In addition, even if an attacker steals k-1 shares, any information about S does not leak out. This means that the SS scheme is secure against both destruction and stealing[2].

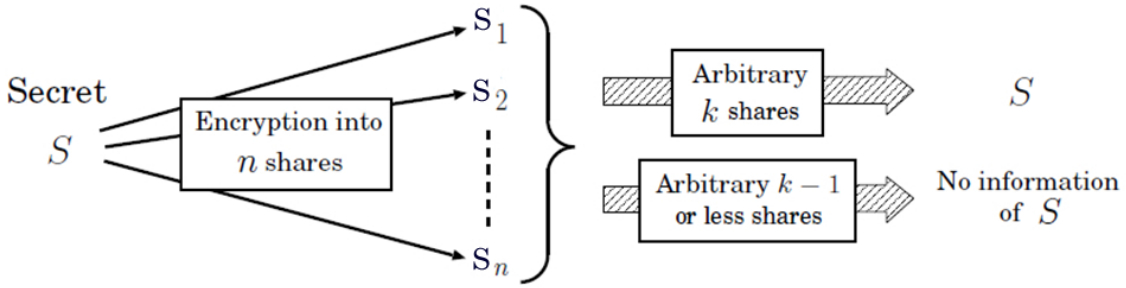


Figure 1: A (k, n)-threshold secret sharing scheme[5].

## III. VISUAL SECRET SHARING

A Visual Secret Sharing (VSS) scheme, which can be named as fundamental principles of visual cryptography proposed by Shamir is a method to encode a secret image into several images (shares), each of which does not reveal any information of the secret image. Each share is printed on a transparency, and is distributed to one of n participants. The secret image can easily be decrypted only by stacking the shares in an arbitrary order. Figure 2 shows how VSS scheme works in reality.

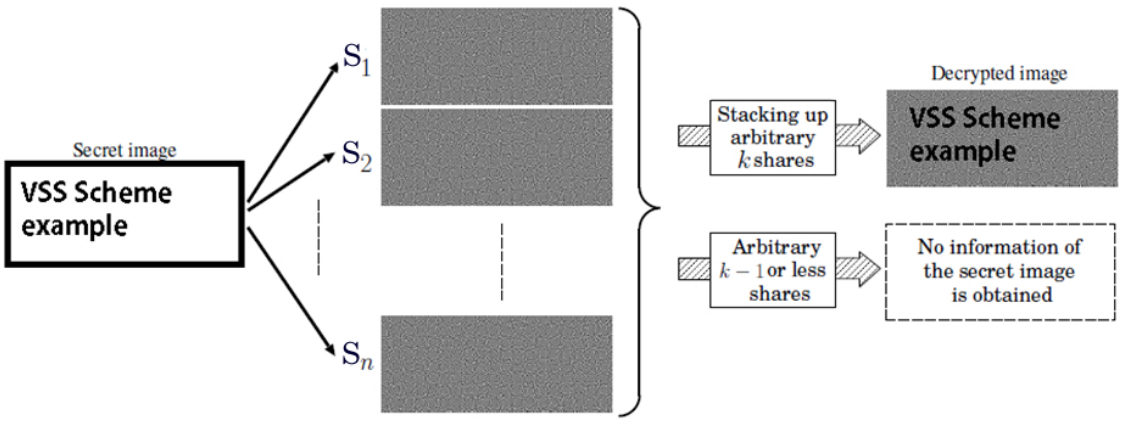


Figure 2: An example of a (k,n)-threshold VSS scheme[5].

# IV. VARIATIONS OF SECRET SHARING SCHEMES

SS schemes introduced in previous sections are based on algebraic calculations in their realizations [8]. But there are some different realizations from ordinal SS schemes. In such other realizations, some physical information are used instead of numbers on finite fields[8]. Table2 shows what kind of secret information is used to realize each SS scheme. In case of images as a secret information the VSS scheme

Table1: Variations of secret sharing schemes[5].

| Based on | Name | Secret information |
|---|---|---|
| Computers | SS schemes | Numbers infinite fields |
| Human sense | Visual cryptography | Images |
| | Cerebral cryptography | 3D images |
| | Optical cryptography | Lights |
| | Audio cryptography | Sounds |
| | Tempo-based audio cryptography | Rhythms |
| Quantum information | Quantum SS scheme | Numbers |
| | Quantum SS scheme | Quantum states |

# V. VISUAL CRYPTOGRAPHY

VC is defined as a process for perfectly encrypting digital data that could be decoded using solely the human visual system[3]. This idea would allow data, in our case images, to be digitally transmitted or stored without concern that the data could be intercepted and accidentally revealed to unauthorized parties. The primary description associated with VC is the message being encoded into two or more shares. When looked at individually, these shares reveal no information about the message contained in them and resemble random noise[4].

# VI. VISUAL CRYPTOGRAPHY PROCESS

The process behind VC is to generate shares randomly based on the input date (image) in such way that the outputs can stack together to show the input. Assuming that the message being encrypted is a binary image with *p* pixels, each of these pixels are separately encoded with a subpixel grouping with *s* pixels[5]. This allows n shares to be generated using these subpixel groupings. Each share is a collection of *m* black and white subpixels. These subpixel groupings are typically square to not distort the aspect ratio of the original image[5]. However, subpixel groupings that are not square do happen in VC algorithms and the aspect ratio of the image is altered accordingly.

This structure can be described as an n×m Boolean matrix S. The structure of S can be described thus: $S = (s_{ij})_{m \times n}$ where $s_{ij} = 1$ or 0 iff the $j^{th}$ sub-pixel of the $i^{th}$ share is black or white.

The important parameters of the scheme are[3]:

- m, the number of pixels in a share.
- α the relative difference in the weight between the combined shares that come from a white and black pixel in the original image (the loos in contrast).
- γ the size of the collection of $C_0$ and $C_1$
- $C_0$= the sub pixel patterns in the shares for a white pixel.
- $C_1$= the sub pixel patterns in the shares for a black pixel.

The Hamming weight H(V) of the ORed m-vector V is interpreted by the visual system as[3]:

- Interpreted as black if $H(V) \geq d$ for threshold d
- Interpreted as white if $H(V) \leq d - \alpha m$ for relative difference $\alpha > 0$
- $1 \leq d \leq m$

The shares can be generated in the following manner:

1. If the pixel of the original binary image is white, randomly pick the same pattern of four pixels for both shares.
2. If the pixel of the original image is black, pick a complementary pair of patterns,

The most commonly used subpixel groupings in VC algorithms are shown in Figure 3. The image is encoded in n shares and the message can be revealed by stacking *k* of those n shares. The generation of the shares is based on the value of the pixel and the probability of a subpixel group occurring[5]. A share generation scheme corresponding to *k=2* and *n=2* is shown in Figure 4. This is applied to a binary image by assigning the corresponding subpixel grouping to the pixels throughout the image. This results in two random shares where the message cannot be identified.

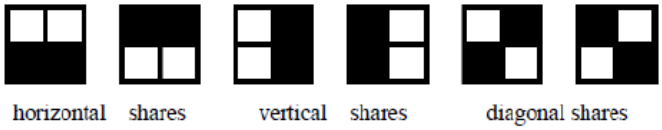


Figure 3: Shares most commonly used for Visual Cryptography[4].

As figure 4 depicts a pixel is divided into four parts, can have six different states. If a pixel on share 1 has a given state, the pixel on share 2 may have one of two states: identical or inverted to the pixel of share 1[4]. If the pixel of share 2 is identical to share 1, the overlaid pixel will be half black and half white. Such overlaid pixel is called grey or empty. If the pixels of share 1 and 2 are inverted or opposite, the overlaid version will be completely black. This is an information pixel. If the pixel states of share 1 are truly (crypto secure) random, both empty and information pixels of share 2 will also have completely random states[4]. One cannot know if a pixel in share 2 is used to create a grey or black pixel, since we need the state of that pixel in share 1 (which is random) to know the overlay result.

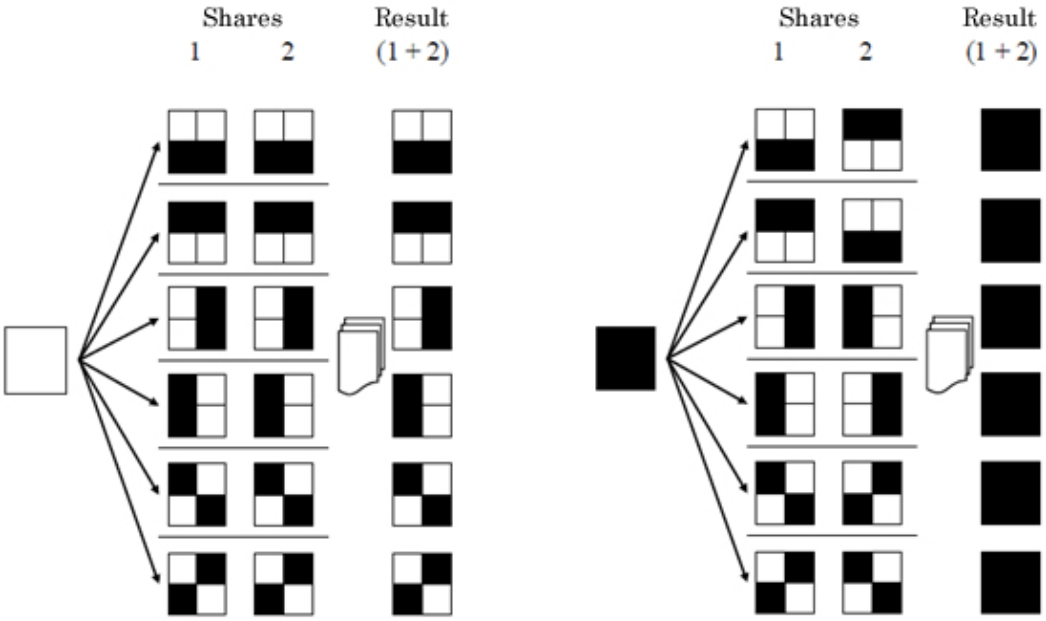


Figure 4: A share generation scheme corresponding to k=2 and n=2[4].

## VII. Extension to Gray and Color Images

The process of VC, as developed through the original algorithm [2], was designed to be used with binary images. As long as the secret messages being encoded can be represented in binary structure, the process shown in the original algorithm works well[4]. However, in reality the world is not composed of solely black and white pixels. With the increasing production of images in the digital age, gray and color images have a pressing need for encryption and protection as much, or more, as binary images[5].

## VIII. Gray Images

Although, Shamir focus most of his paper on the development of an algorithm to encrypt binary images he was also aware of the eventual need to encrypt gray and color images so he proposed a technique which involved printing each of the pixels in an image as half black - half white circles[5]. This allowed the rotation angle of the

corresponding circles to vary and which would reveal a range of gray tones throughout the overlapped shares. If the rotation angle of the first share pixels are chosen at random, then the relative change in rotation of the corresponding share pixels would result in uniformly gray shares with no information about the original image being revealed [4]. An example of this process is shown in Figure 5 which illustrates the overlapping circle pixels process.

While this process has not been popular for encrypting gray images, there has been growing research on other techniques that have gained popularity and success among the VC community[4]. One of the more popular methods has implemented the process of halftoning images [4]. Halftoning can be accomplished by thresholding the image. This is done by designating a pixel cut-off value to determine if a gray pixel should be assigned to a black or white pixel[5]. This technique is assigning all gray values below 128 digital counts to black and any above that threshold to white[5]. Another approach is to examine a subgroup of pixels, determine their average, and reassign that block of pixels with a designated ratio of black and white pixels approximating that level of gray[4]. The number of gray levels used determine the quality of the resulting black and white (gray) image. To illustrate, Figure 6 shows the original image of Lena and corresponding


Figure 5:Shamir approach to deal with gray images[5].

thresholded images using two, eight, and sixteen gray levels, respectively[6]. By comparing the original image with two, eight and sixteen gray level we can reach to this fact that the sixteen gray levels is the best representation of the original image but the two gray level image shows the overall shape of the image and major features but does not show more details. The eight gray level image shows more detail than the two level image but still blurs some of the edges and gives false shadows. It is obvious that having more levels of gray needs additional time for processing but the output would have a good contrast and it would be more representative in comparison with lower levels of gray.

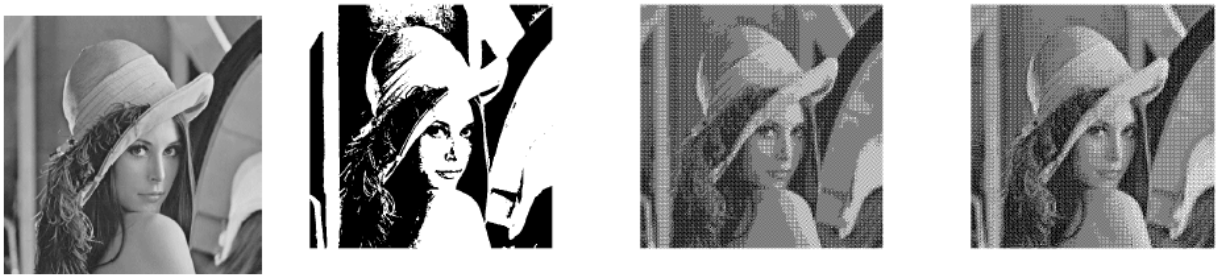

Figure 7: two, eight and sixteen gray levels[5].

## IX. Color Images

Having images in the world cannot be solely represented by binary or gray images. The real life is dealing with colorful images. The method uses the procedure illustrated in figure. 8 to transform a color secret image into three C, M, and Y halftone images. Then, every pixel of the halftone images is expanded into a 2×2 block. Every block of the sharing images therefore includes two transparent (white) pixels and two color pixels[4]. There is also a half black-and-white mask to shade unexpected colors on the stacked sharing images so that only the expected colors show up.

In figure 9 . If pixel Pij of the composed image is (0, 0, 0), the distribution of the color pixels in the three sharing images is assigned as the first row in figure. 9. After stacked by the mask image, all the color pixels on the three sharing images are shaded by black pixels and only the white pixels can reveal, thus showing a white-like color. If pixel Pij is (1, 1, 0), only the C and M components are revealed, with the Y component being covered by the black mask[4]. The distribution of the color pixels in the three sharing images is as the fifth row in figure. 9, thus showing a blue-liked (cyan plus magenta) color. If pixel Pij is (1, 1, 1), the C,M, and Y parts can all be revealed, thus showing a black color[4]. The distribution of the color pixels in the three sharing images is as the eighth row

in figure. 9. The eight combinations of the three primary colors of the composed image under this method are illustrated in figure. 9. Moreover, we can also analyze the color distribution of the stacked image in terms of color quantity. For example, the first row in figure. 9 shows that black color occupies half of the 2×2 block in the composed image[9]. Since black can be seen as the composition of C, M, and Y, which means that C, M, and Y occupy half of the whole block respectively, the densities of C, M, and Y components within a 2×2 block are all $\frac{1}{2}$ [6]. If the distribution of color pixels in the composed image is as the fifth row in figure. 9, only C and M are revealed with Y being covered by the black mask. Since black can be seen as the composition of C, M, and Y, C and M can appear in all four blocks of a 2×2 block in the composed image, but yellow only appears in two. So the color intensity of C, M and Y can be denoted as $(1, 1, \frac{1}{2})$[6]. If the distribution of color pixels in the composed image is as the eighth row in figure. 9, four blocks are all black and the color intensity (C, M, Y) can be denoted as (1; 1; 1). As a result, white pixels in a stacked image are no longer pure white (0; 0; 0), but are half black-and-white$(\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$ instead. Accordingly, the colors in a stacked image are no longer distributed between (0; 0; 0) and (1; 1; 1), but are distributed between $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$ and (1, 1, 1)[6].

.

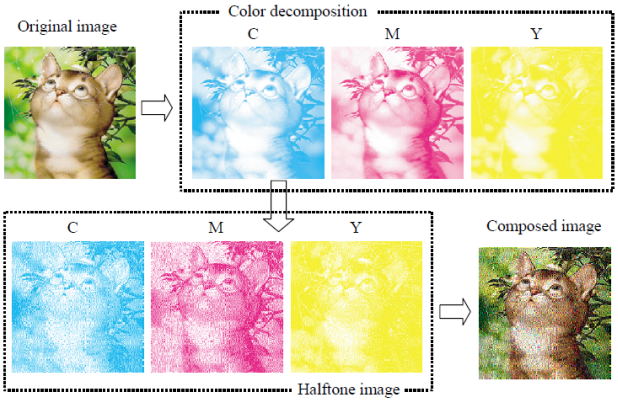


Figure8: transforming a colorful secret image into three C, M, and Y halftone images [6].

| Mask | Revealed color (C,M,Y) | Share1(C) | Share2(M) | Share3(Y) | Stacked image | Revealed color quantity (C,M,Y) |
|---|---|---|---|---|---|---|
| | (0, 0, 0) | | | | | (1/2, 1/2, 1/2) |
| | (1, 0, 0) | | | | | (1, 1/2, 1/2) |
| | (0, 1, 0) | | | | | (1/2, 1, 1/2) |
| | (0, 0, 1) | | | | | (1/2, 1/2, 1) |
| | (1, 1, 0) | | | | | (1, 1, 1/2) |
| | (0, 1, 1) | | | | | (1/2, 1, 1) |
| | (1, 0, 1) | | | | | (1, 1/2, 1) |
| | (1, 1, 1) | | | | | (1, 1, 1) |

Figure 9: Visual Cryptography Scheme for Color Images Using CMY Subpixels[6].

## X. Visual Cryptography and its Applications in the Real World

Lots of algorithms and approaches based on visual cryptography have been proposed and as we expect they are trying to address security issues in communications. For example, in [27] Visual Cryptography has been applied for authentication for Data Matrix Code in Identity cards and Sherafat [14] mentioned it as one of the criterial that can be considered in web site evaluation. Tunga in [28] proposed a scheme that describes a safety mechanism based on Visual Cryptography. The mechanism described consists of a lock and a key. For every pair of lock and key there is a unique image associated. The unique image is even unknown to the owner of the lock and key that can be applied in [8,11,12,18, 20]. Beside the mentioned approaches there are lots of potentional applications for visual cryptography in banking with respect to authentication and authorization[9].

# XI. Conclusion

Visual cryptography is one the secure ways to transfer and store digital data. The main advantage of visual cryptography is that no computation required to decrypt the final result. It gives this chance to anyone, who has a little knowledge about cryptography, to go through the decryption processing easily. The most important part of any VC scheme is the contrast of the recovered secret from a particular set of shares, as it is not going to be the same as the input image. So there is still room for developing more efficient ways to address this problem.

# References


[1] Naor, Moni, and Adi Shamir. "Visual cryptography." *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer Berlin Heidelberg, 1994.

[2] Lin, Chang-Chou, and Wen-Hsiang Tsai. "Visual cryptography for gray-level images by dithering techniques." *Pattern Recognition Letters* 24.1 (2003): 349-358.

[3] Lin, Chang-Chou, and Wen-Hsiang Tsai. "Secret image sharing with steganography and authentication." *Journal of Systems and software* 73.3 (2004): 405-414.

[4] Naor, Moni, and Adi Shamir. "Visual cryptography II: Improving the contrast via the cover base." *International Workshop on Security Protocols*. Springer Berlin Heidelberg, 1996.

[5] Walden, Disa E. *A Benchmarking assessment of known visual cryptography algorithms*. Diss. Rochester Institute of Technology, 2012.

[6] Hou, Young-Chang. "Visual cryptography for color images." *Pattern Recognition* 36.7 (2003): 1619-1629.

[7] Salisbury, W. David, et al. "Perceived security and World Wide Web purchase intention." *Industrial Management & Data Systems* 101.4 (2001): 165-177.

[8] Rosenberg, Jothy, and David Remy. *Securing Web Services with WS-Security: Demystifying WS-Security, WS-Policy, SAML, XML Signature, and XML Encryption*. Pearson Higher Education, 2004.

[9] He, Warren, et al. "Shadowcrypt: Encrypted web applications for everyone." *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014.

[10] Reddy, L. Siva, and Munaga VNK Prasad. "Extended Visual Cryptography Scheme for Multi-secret Sharing." *Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics*. Springer India, 2016.

[11] Jalili, Reza. "Secure data entry and visual authentication system and method." U.S. Patent No. 6,2009,104. 27 Mar. 2001.

[12] Banik, Barnali Gupta, and Samir Kumar Bandyopadhyay. "Secret sharing using 3 level DWT method of image steganography based on Lorenz chaotic encryption and visual cryptography." *Computational Intelligence and Communication Networks (CICN), 2015 International Conference on*. IEEE, 2015.

[13] Russ, John C. *The image processing handbook*. CRC press, 2016.

[14] Sherafat, A., A. Pouriyeh, and M. Doroodchi. "EV-IMP Model: A comprehensive model for evaluation of an organization's website success." *Proceedings of the International Conference on Semantic Web and Web Services (SWWS)*. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2013.

[15] Arafin, Md Tanvir, and Gang Qu. "Secret Sharing and Multi-user Authentication: From Visual Cryptography to RRAM Circuits." *Proceedings of the 26th edition on Great Lakes Symposium on VLSI*. ACM, 2016.

[16] Martin, V. Maria Antoniate, K. David, and P. Mesiya. "A Survey on Visual Secret Sharing Scheme." *Software Engineering and Technology* 8.4 (2016): 91-96.

[17] Nordbotten, Nils Agne. "XML and web services security standards." *IEEE Communications Surveys & Tutorials* 11.3 (2009): 4-21.

[18] Pouriyeh, Seyed Amin, and Mahmood Doroodchi. "Secure SMS Banking Based On Web Services." *SWWS*. 2009.

[19] Garfinkel, Simson, and Gene Spafford. *Web security, privacy & commerce*. " O'Reilly Media, Inc.", 2002.

[20] Akhawe, Devdatta, et al. "Towards a formal foundation of web security." *2010 23rd IEEE Computer Security Foundations Symposium*. IEEE, 2010.

[21] Pouriyeh, Seyed Amin, Mahmood Doroodchi, and M. R. Rezaeinejad. "Secure Mobile Approaches Using Web Services." *SWWS*. 2010.

[22] Benzel, Terry. "The IEEE Security and Privacy symposium workshops." *IEEE Security & Privacy* 14.2 (2016): 12-14.

[23] Wahab, Omar Abdel, et al. "A survey on trust and reputation models for Web services: Single, composite, and communities." *Decision Support Systems* 74 (2015): 121-134.

[24] Dalvand, Babak, Saeed Safaei, and Mojtaba Nazari. " Fast Parallel Molecular Solution to the Maximum Triangle Packing Problem on Massively Parallel Bio-Compting ." *FCS*. 2009.

[25] Soutar, Colin, et al. "Biometric encryption using image processing." *Photonics West'98 Electronic Imaging*. International Society for Optics and Photonics, 1998.

[26] Ko, Teddy. "A survey on behavior analysis in video surveillance for homeland security applications." *2008 37th IEEE Applied Imagery Pattern Recognition Workshop*. IEEE, 2008.

[27] Sharma, M. Agnihotra, and M. Chinna Rao. "Visual cryptography authentication for data matrix code." *International Journal of Computer Science and Telecommunications* 2.8 (2011): 58-62.

[28] Tunga, Harinandan, and Soumen Mukherjee. "Design and Implementation of a Novel Authentication Algorithm for Fool-Proof Lock-Key System Based On Visual Secret Sharing Scheme." *IJCSI International Journal of Computer Science Issues* 9.3 (2012).

[29] Blundo, Carlo, Alfredo De Santis, and Moni Naor. "Visual cryptography for grey level images." *Information Processing Letters* 75.6 (2000): 255-25

PeerJ Preprints | https://doi.org/10.7287/peerj.preprints.2682v1 | CC BY 4.0 Open Access | rec: 3 Jan 2017, publ: 3 Jan 2017