International Journal of Engineering Research and General Science Volume 3, Issue 2, Part 2, March-April, 2015
ISSN 2091-2730

Protecting Documents Using Visual Cryptography

Ali J. Abboud

University of Diyala _College of Engineering, ali.j.abboud@uodiyala.edu.iq

Abstract— Digital documents are produced in enormous amounts everywhere in the digital world. The confidentiality, authenticity and integrity of these documents increased dramatically recently in the insecure networked environments. In this paper, we design new methods based on the visual cryptography and steganography to protect multiple digitized documents from threats created by unauthorized people. Visual cryptography is a visual secret sharing scheme used widely and proved to be secure enough in different areas. The experimental results demonstrate the efficacy of these methods to protect sufficiently multiple digital documents.

Keywords: visual cryptography, secret sharing, multiple documents protection, LSB, confidentiality, integrity and authentication.

I. INTRODUCTION

In the internet era, all our daily life actions have been managed electronically using huge number of computers connected by internet network. These electronic actions include selling and buying different things, online managing of bank accounts, online booking of air flight tickets, registering in the universities and schools and online applying for visa [1]. All these activities need to produce and manage documents digitally, an example on these documents, including university transcripts, letters and business contracts [2]. Producing digital documents electronically is more convenient and simpler than paper documents and also dealing with paperless documents is far better because of the ease of editing, searching and storing of them [1]. In addition, making these documents available digitally in the computer networks permit them to be transmitted and processed electronically [2]. However, releasing documents in the networks exposes them to different types of attacks and threats, hence; protecting digital documents is very important matter in the networked society [3].

Recently, several approaches have been proposed to protect documents. Fischer and Herfet [2] proposed a technique to protect documents integrity using visual CAPTCHAs and compared it with different kinds of authentication mechanisms such as digital signatures and hash functions. Same authors in [2] developed another method to provide document authentication using human-recognizable watermarks instead of digital signatures and message authentication codes that need complex computations [3]. Fischer and Herfet continued to improve their proposed methods explained earlier by adding text transformations to make document authentication more robust. The rest of paper is organized as follows: in section **II** visual cryptography concepts are explained, section **III** is devoted to explain our proposed methods thoroughly and finally section **IV** is dedicated for conclusions and future work.

II. VISUAL CRYPTOGRAPHY

Visual cryptography is a methodology proposed by Naor and Shamir in 1994 to share secret information among several participants in the shape of transparencies [4]. The secret information may be handwritten notes, images or text that can be uncovered without any complex cryptographic computations [4]. In the (**k, n**) visual cryptographic scheme, the secret information is shared among **n** participants and the secret is recovered if **k** or more shares (or transparencies) stacked together. Otherwise, if **k-1** or fewer of shares are available only then we cannot reveal secret information. In the following, we describe the main schemes of visual cryptography as follows:

A. Black and White Visual Cryptography Scheme [2, 4, 5]

In black and white visual cryptography scheme, every pixel in the secret image is partitioned into 2x2 block in the two shares based on the rules in the **Fig. 1**. If white pixel exist in the secret image, then the dealer choose randomly one of shares in the first row and distribute them on shared transparencies; otherwise if the color of secret image is black, then the dealer choose randomly one of the shares in the second row and distribute them on the shares. Furthermore, the results of stacking sub-pixels in the shared transparencies: black and black is black, black and white is black, white and white is white. Finally, when the dealer stack two transparencies together, stacking black blocks give full black color and stacking white blocks gives half black and half white.

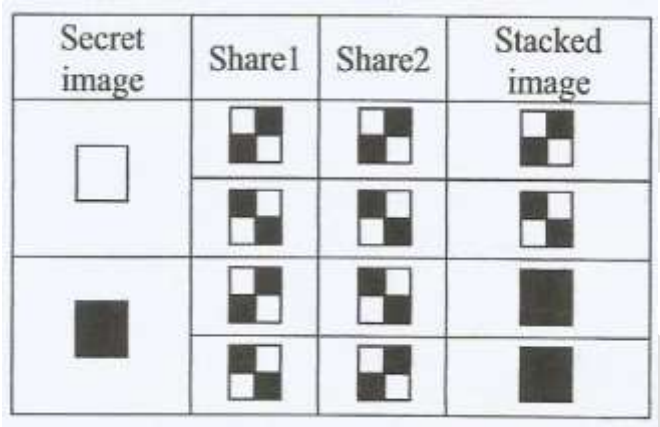

Figure (1): Black and white visual cryptography scheme [5].

B. Gray-level Visual Cryptography Scheme [5, 6, 7]

Gray-level visual cryptography scheme is a developed version of black and white counterpart. In this scheme, halftoning technology is used to convert gray image into black and white image to be later encoded by dealer. Halftoning is a widely employed in the printers and scanners to convert continuous tone image to halftone image. The algorithm of gray-level visual cryptography scheme [5]:

1. Transform the gray-level image into a black-and-white halftone image.
2. For each black or white pixel in the halftone image, decompose it into a 2x2 block of the two transparencies according to the rules in the **Fig. 1**. If the pixel is white, randomly select one combination from the former two rows in **Fig.1** as the content of blocks in shares 1 and 2. If the pixel is black, randomly select one combination from the latter two rows as the contents of the blocks in the two transparencies.
3. Repeat step 2 until every pixel in the halftone image is decomposed, hence resulting in two transparencies of visual cryptography to share the secret image.

C. Color Visual Cryptography Scheme [5]

Y.-C. Hou [4] developed three methods for color visual cryptography. All these methods use CMY (**C**= Cyan, **M**= Magenta, **Y**= Yellow) color model to decompose and halftoning color images as shown in the **Fig. 2**.

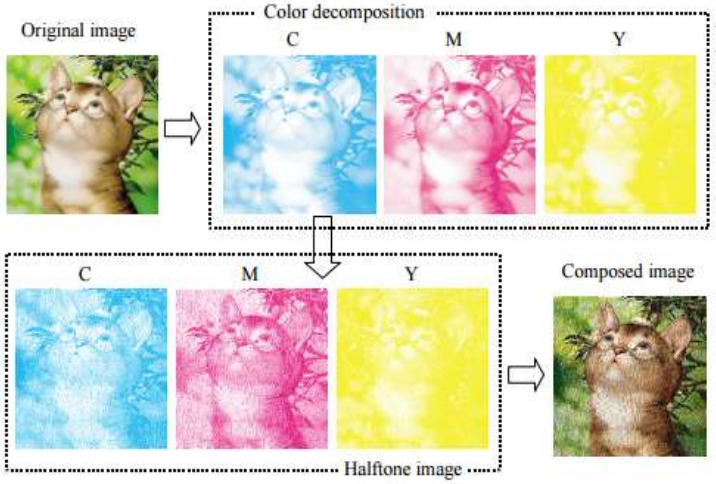

Figure (2): color image decomposition and halftoning [5].

Method 3 of Hou [5] is adopted in our paper as shown in the **Fig. (3).** Its algorithm is described below:

1. Transform the color image into three halftone images: C, M, and Y.
2. For each pixel P_{ij} of the composed image, do the following:
   (a) According to the traditional method of black-and-white visual cryptography, expand C_{ij}, M_{ij} and Y_{ij} into six 2×2 blocks, $C1_{ij}$; $C2_{ij}$; $M1_{ij}$; $M2_{ij}$ and $Y1_{ij}$, $Y2_{ij}$.
   (b) Combine the blocks $C1_{ij}$, $M1_{ij}$ and $Y1_{ij}$ and fill the combined block corresponding to P_{ij} in Share 1.
   (c) Combine the blocks $C2_{ij}$, $M2_{ij}$ and $Y2_{ij}$ and fill the combined block corresponding to P_{ij} in Share 2.
3. Repeat Step 2 until every pixel of the composed image is decomposed, hence obtaining two visual cryptography transparencies to share the secret image.
4. After stacking the two sharing images, the secret image can be decrypted by human eyes.

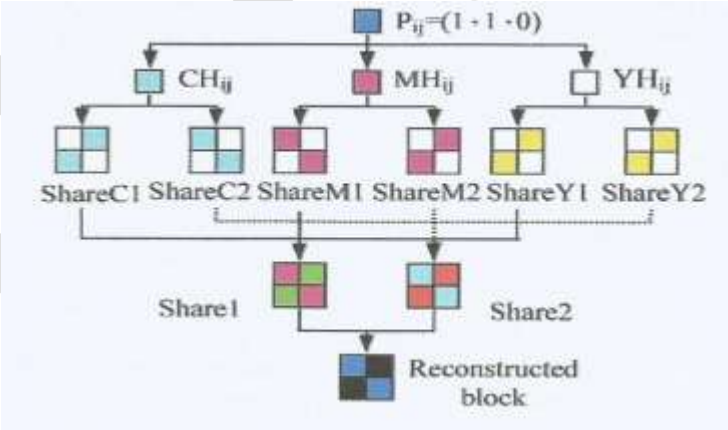

Figure (3): Color visual cryptography scheme_ Method 3 [5].

III. MULTIPLE DOCUMENTS PROTECTION METHODS

The proposed schemes to digital document authentication [1, 2, 3] are focused only on the integrity of them with no consideration to the number of documents or their size. In our proposed methods, we show how to protect several digital documents by using visual cryptography and the least significant bit (LSB) steganography method. LSB is data hiding methodology used to protect secret data

from unauthorized access by embedding bits of secret data (such as digital document image) inside the least significant bits of preselected cover image [6]. The proposed methods are:

A. Method 1

Multiple Documents Secret Sharing

1. Select the color cover image (**C**) to be used to contain all color document images. It should be large enough to have them.
2. Specify the number of document images (**NoD**) to be hided in **C.** Also, the number of bits of each pixel in the **C** to be used to embed the bits of document images **NoD**.
3. Determine the percentage of used pixels of **C** by **NoD image** pixels, if their percentage greater than (100%) then we should reduce the **NoD,** otherwise continue in the method.
4. Use method3 of Hou [4] explained previously to do color visual cryptography on the cover image **C** to obtain two shares (**share1** and **share2**).
5. Use **LSB** steganography method to hide the pixel bits of **NoD images** inside pixel bits of **share1** or **share2** or distribute **NoD** document images between two shares**.**
6. Distribute **share1** and **share2** to two participants or combine two shares to obtain expanded cover image **C1**.

Multiple Documents Secret Recovery

1. If we have two shares of C then the pixel bits of all embedded documents can be recovered exactly from where they are embedded in either **share1** or **share2.**
2. If we have **C1, then** we can separate it into two shares **share1** and **share2** and do what we did in step 1 to recover secret documents.

B. Method 2

Multiple Documents Secret Sharing

1. Select the color cover image (**C**) to be used to contain all color document images. It should be large enough to have them.
2. Specify the number of document images (**NoD**) to be hided in **C.** Also, the number of bits of each pixel in the **C** to be used to embed the bits of NoD image pixels.
3. Determine the percentage of used pixels of **C** by **NoD images** pixels, if the percentage greater than (100%) then we should reduce the **NoD,** otherwise continue in the method.
4. Use method3 of Hou [4] explained previously to do color visual cryptography to the cover image **C** and **all** document images to obtain two shares (**share1** and **share2**) for each one of them.
5. Use LSB steganography method to hide the pixel bits for the **share1 of NoD** document images inside pixel bits of **share1 of C** and similarly hide the pixel bits for the **share2 of NoD** inside pixel bits of **share2 of C.** In addition**,** we can embed shares of document images inside any share of **C.**
6. Distribute **share1** and **share2** to two participants or combine two shares to obtain expanded cover image **C1**.

Multiple Documents Secret Recovery

1. If we have two shares of C then the pixel bits of all embedded documents can be recovered exactly from where they are embedded in either **share1** or **share2.**
2. Reform share1 and share2 of all document images.
3. Decrypt document images by combining share1 and share2 of each document image.
4. If we have **C1,** then we can separate it into two shares **share1** and **share2** and do what we did in steps (1, 2, and 3) to recover secret documents.

The results of applying method 1 and method2 to set of three document images are shown in the **Fig. (4)** and **Fig. (5)** respectively.

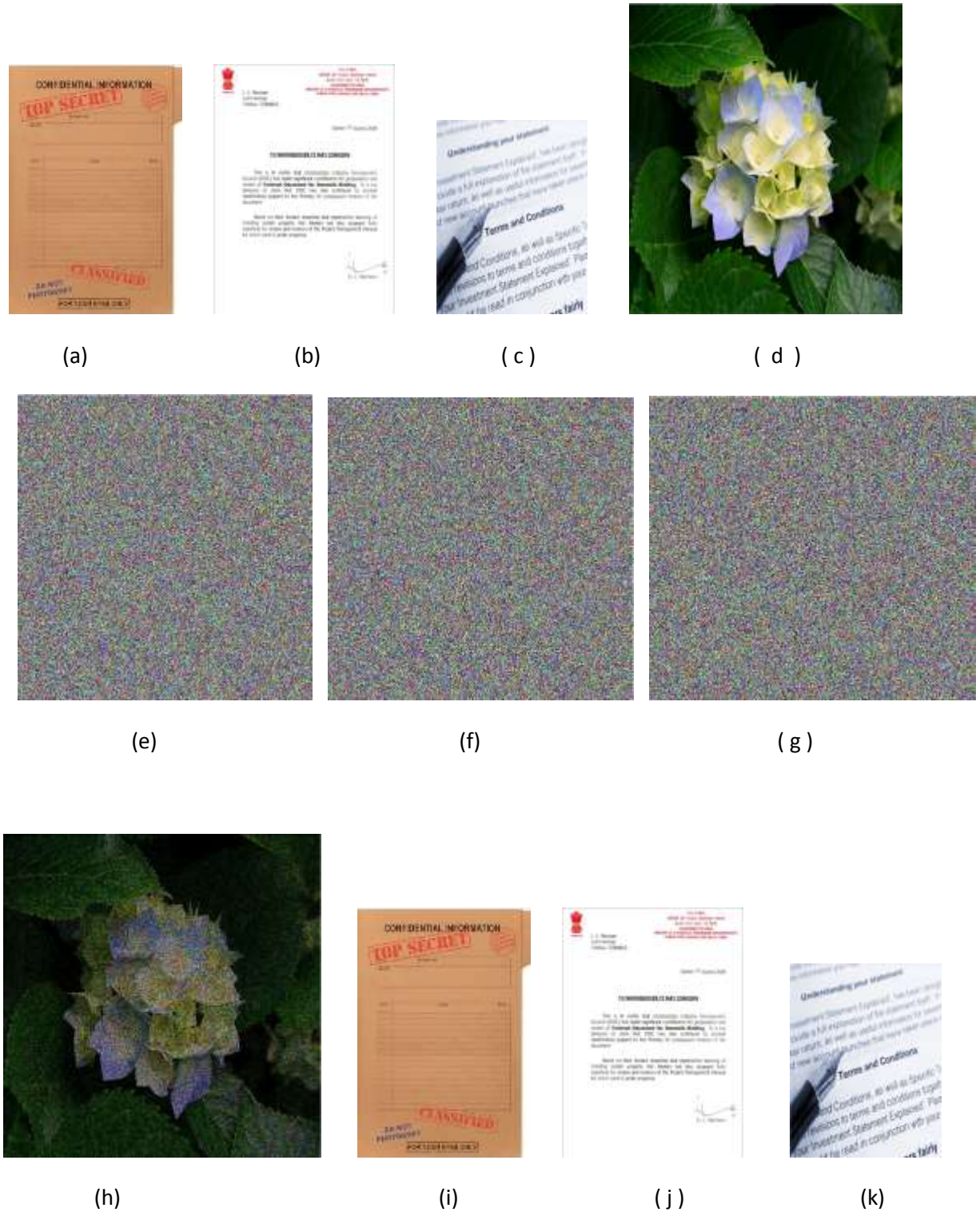

Figure (4)_ method1: (a) Document1 before hiding (b) Document 2 before hiding (c) Document 3 before hiding
(d) Cover image before visual cryptography (e) Share1 of cover image after hiding document images
(f) Share1 of cover image after visual cryptography (g) Share2 of cover image after visual cryptography
(h) Cover image after overlapping two shares (i) Document1 after extraction
(j) Document2 after extraction (k) Document3 after extraction

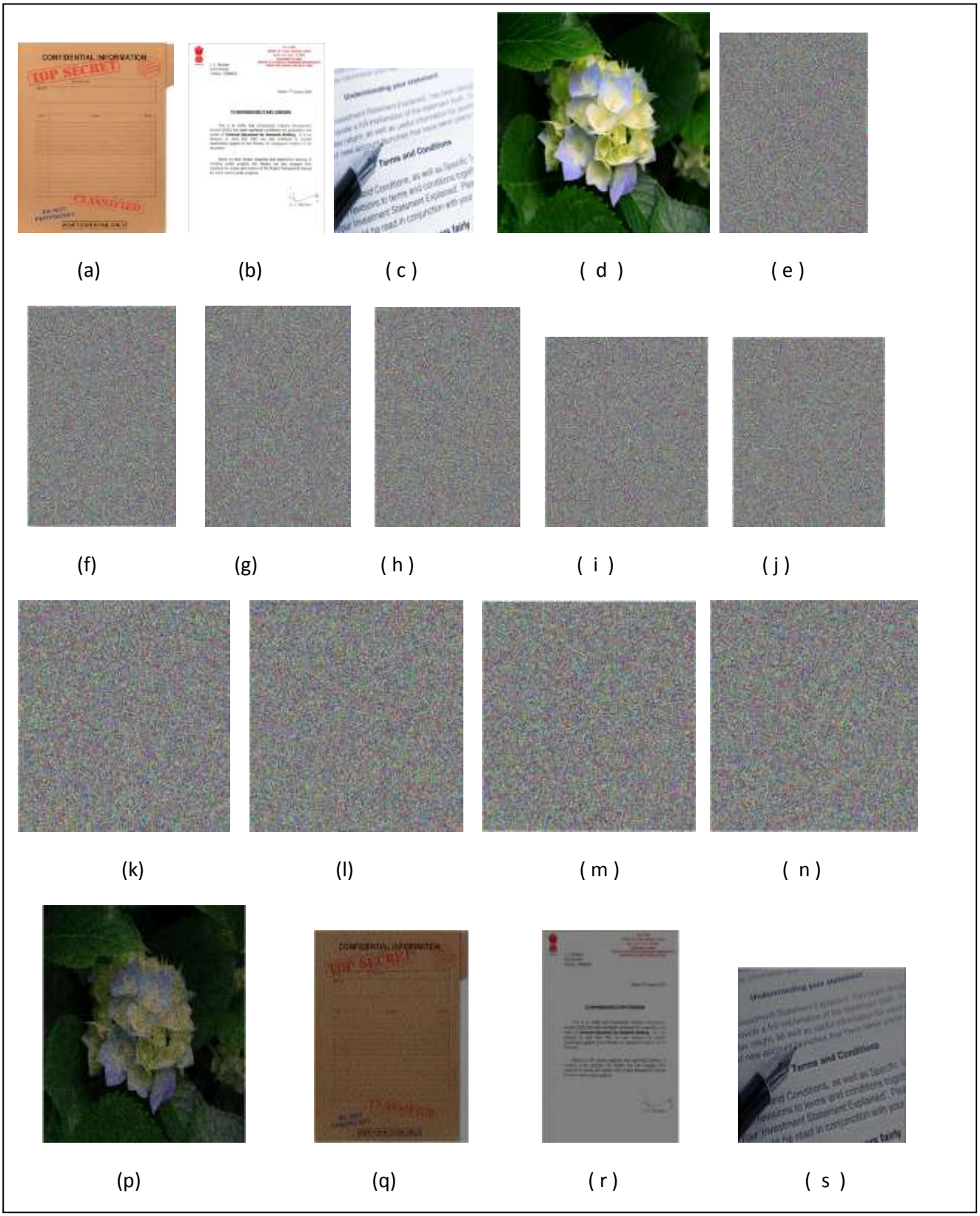

Figure (5)_method2: (a) Document1 before hiding (b) Document 2 before hiding (c) Document 3 before hiding
(d) Cover image before visual cryptography (e) Share1 of document 1 (f) Share2 of document 1
(g) Share1 of document 2 (h) Share2 of document 2 (i) Share1 of document 3 (j) Share2 of document 3
(k) Share1 of cover image before hiding (l) Share2 of cover image before hiding (m) Share1 of cover image after hiding

(n) Share2 of cover image after hiding (p) Cover image after overlapping shares
(q) Document1 after extraction (r) Document2 after extraction (s) Document3 after extraction

IV. CONCLUSIONS AND FUTURE WORK

In this paper, we developed new methods to protect multiple digital documents simultaneously. The first method provides acceptable security with good document image quality. However, the second method provides strong security with some degradation in the document image quality after extraction. As future work, we can make the following suggestions:

1. Use other steganography techniques.
2. Use biometrics [8, 9, 10, 11, 12], watermarks and other cryptography algorithms.
3. Developing comprehensive security methods that include integrity, authentication and confidentiality [13, 14, 15].
4. Developing authentication techniques for documents in cloud computing infrastructures [16].

To sum up, this paper represents initial study to design more efficient and robust information security mechanisms in the insecure networked environments.

REFERENCES:

[1] Fischer, Igor, and Thorsten Herfet. "Watermarks and text transformations in visual document authentication", Journal of Computers 2.5, 44-53, 2007.
[2] I. Fischer and T. Herfet, "Visual CAPTCHAs for document authentication," in Proceedings of the IEEE International Workshop on Multimedia Signal Processing (MMSP). IEEE, pp. 471–474, October 2006.
[3] I. Fischer and T. Herfet, "Visual document authentication using human-recognizable watermarks," in Proceedings of ETRICS 2006, LNCS 3995. Springer-Verlag, pp. 509–521, June 2006.
[4] M. Naor, A. Shamir, Visual cryptography, Proc. Eurocrypt '94, LNCS 950, 1–12,1994.
[5] J.C. Hou, Visual cryptography for color images, Pattern Recognition, 36 (7), 1619–1629, 2003.
[6] Juneja, M., Sandhu, P. S. "Improved LSB based Steganography Techniques for Color Images in Spatial Domain", IJ Network Security, 16(4), 366-376, 2014.
[7] Blundo, C., De Santis, A., Naor, M., "Visual cryptography for gray level images", Information Processing Letters, 75, 255–259, 2000.
[8] A.J. Abboud, H. Sellahewa and S.A. Jassim, "Image quality approach for adaptive face recognition", in Proc. Mobile Multimedia / Image Processing, Security and Applications, SPIE, vol.7351,pp. 1-10, 2009.
[9] S. A. Jassim, H. Al-Assam, A. J. Abboud, and H. Sellahewa. Analysis of Relative Entropy, Accuracy, and Quality of Face Biometric. Pattern Recognition for IT security Workshop, 2010.
[10] Hisham Al-Assam, Ali Abboud, Harin Sellahewa, and Sabah Jassim. "Exploiting relative entropy and quality analysis in cumulative partial biometric fusion." In Transactions on Data Hiding and Multimedia Security VIII, pp. 1-18. Springer Berlin Heidelberg, 2012.
[11] A.J. Abboud and Sabah A. Jassim. "Biometric templates selection and update using quality measures." In SPIE Defense, Security, and Sensing, pp. 840609-840609. International Society for Optics and Photonics, 2012.
[12] A. J. Abboud and Sabah A. Jassim. "Image quality guided approach for adaptive modelling of biometric intra-class variations." In SPIE Defense, Security, and Sensing, pp. 77080L-77080L. International Society for Optics and Photonics, 2010.
[13] Al-Assam, H., Ali Abboud, and Sabah Jassim. "Hidden assumption of face recognition evaluation under different quality conditions." In Information Society (i-Society), 2011 International Conference on, pp. 27-32. IEEE, 2011.
[14] Al-Assam, Hisham, Ali Abboud, and Sabah Jassim. "Exploiting Samples Quality in Evaluating and Improving Performance of Biometric Systems", International Journal of Digital Society (IJDS), Volume 2, Issue 2, June 2011.
[15] A.J. Abboud and Sabah A. Jassim. "Incremental fusion of partial biometric information." In SPIE Defense, Security, and Sensing, pp. 84060K-84060K. International Society for Optics and Photonics, 2012.
[16] Ali J Abboud and Omar S Saleh," Sustainable IT: A Realisation Survey among Academic Institutions of Iraq", International Journal of Enhanced Research in Science Technology & Engineering, Vol. 3 Issue 2, pp. (25-31), 2014