Blocks - Based Data Hiding Approach for Electronic Cheque Authentication

Hiba Z. Zeydan
College of Political, Al-Nahrain University, Baghdad-Iraq.
E-mail: perla_hzz26@yahoo.com.

Abstract

This research, suggests a combination of digital representation and authentication methods to electronically transfer the typical paper-based bank cheque between banks over open and insecure computer networks like Internet. This proposed combination would be a sender – receiver protocol. At the sender side, a scanned colored image of the bank cheque would be transformed to a binary image, and a sequence of bits would be extracted from it and embedded back into it again as a content-dependent authentication signature (AS) which would be computed by using some image data and a secret key. At the receiver side, the AS would be extracted from the signed binary cheque image (the host image) in order to verify the cheque's authenticity; and to locate any illegal alterations that may be done in the host image by malicious hackers during the transmission. Both AS extraction and embedding methods are blocks-based methods in order to locate the exact blocks where the undesirable modifications may be done in the host image. Some experimental results and mathematical metrics would be tested to demonstrate the validity of the suggested data hiding approach. The conclusions would show that this suggested approach can be used to electronically sign the binary cheque image without causing noticeable loss of its visual quality; and with much storage and band saving during the electronic transfer between the sender and the receiver.

Keywords: Data Hiding, AWT, E-cheque, AS, Ready Blocks, ASR, NASR.

Introduction

With the rapid growth of open computer networks like Internet and the latest advances in digital technologies, a huge amount of digital images is being exchanged over Internet. It is often true that a large part of these images is confidential, private or both, which increases the demand for stronger protection and authentication schemes [1]. *"Data Hiding"* schemes are the preferred techniques for protecting the transmitted image data [2]. A "*Data Hiding*" scheme means a technique to embed a sequence of bits in a host image with small visual aspect and to extract it afterwards [3]. as a result, there are various data hiding techniques for image authentication, and it can be urged that there is no single data hiding technique satisfies the different image types (continuous tone, halftone and binary image types) [4, 5]. *"Authentication Watermarking Technique"* or *AWT* is a form of data hiding occurs when some unique data is imprinted inside the image. *AWT* is the process that inserts hidden data into an image, in order to detect any accidental or malicious image alterations [6, 7]. In *AWT*, an "*authentication signature"* or *AS* is computed from the whole image and inserted into the image itself. Thus, an *AS* contains information about the host image - so that it is thought to be content dependent- that may be checked to verify the image's integrity and authenticity. Furthermore, *AWT* is basically fragile because *AS* can be easily removed and detected to report the corruption of the image correctly [3, 6]. "*Electronic cheque*" or "*E-cheque*" is a good example of those applications use *AWT* to maintain bank cheque confidentiality and authenticity between the sender and the receiver. *E-cheque* is the substitution of physical exchange of paper-based bank cheque by the electronic exchange of cheque image over Internet, so that it brings agility, security and cost reduction to the clearing bank systems [8]. Because the binary image brings great memory saving and text legibility [8], and the use of typical image compression techniques at high rates may strongly alter the textual parts which does the cheque image have [9]. Thus, this research suggests a combined approach which combines two methods: representation and authentication methods for the *E-cheque*. The representation method involves converting the scanned color cheque image into binary image-black and white image as a solution to

preserve the textual content legibility of cheque image. And the authentication method involves blocks based *AWT* whose main idea is: to divide binary cheque image into small (3×3) blocks and to prioritize them by matching with predefined patterns, in order to embed an *AS* into the binary cheque image itself without changing its visual aspect. Furthermore, this combined approach cannot only verify the authenticity of cheque image, but also can locate the illegal modifications. The rest of this research is organized as follows. Section 2 presents a historical view of related works. Section 3 describes the proposed combined method in details. Section 4 demonstrates the results and discussion. Finally, section 5 concludes the research.

Background

In the literature, there are many data hiding schemes for continuous tone images. Also, there are many papers on data hiding for binary images but there are no *AWT*s [10, 11, 12]. In [10], the ratio of black versus white pixels was used. Although the algorithm aimed at robustly hiding information in binary image, it was not directly applied for authentication or other fragile use. In [11], the hidden data could not be correctly extracted and the original image might be failed to be recovered perfectly. In [12], an interesting data hiding technique which was named as "data hiding by template ranking" or *DHTR*, has been recently discovered by De Queiroz et al. it has been applied to watermark binary images with excellent visual quality. This *DHTR* –based watermarking method involves: dividing binary image into 8×8 sub-blocks, so only few pixels would be modified and the positions of those pixels and their containing sub-blocks would be known both in the insertion and extraction phases. This method has flipped only low visibility pixels to hide the information (or a watermark) and consequently the watermarked image would have good visual quality. Thus, this method can be used to verify whether a binary image has been tampered or not, and to authenticate its originator. For e-cheque representation, an early paper proposes "mixed raster code" or MRC model for representing and exchanging bank cheque images. This proposal has consisted in binarizing the scanned cheque image, compressing image planes using MRC model and protecting them with digital signature. First, the binary image has been sent from sender to receiver, and the other MRC image planes (foreground and background) have been sent to the receiver to reconstruct the original color bank cheque image. But the use of MRC model has two problems: the border of the text in the reconstructed image at the receiver side would not be sharp, and there would be halos around the border of the text, which might hinder the compression. Also, the electronic transfer of cheque by using this MRC model would not be viable because it would spend more time [8]. This research proposes a combined approach which combines the advantages of both the previously mentioned methods: the binarization and the *DHTR* –based watermarking ideas for both e-cheque representation and authentication. The binarization idea is used to generate an e-cheque model for electronic exchange between sender and receiver, and an extended idea depends on *DHTR* for binary image is used to embed and extract a content based signature as an authentication feature. Not only can this proposed approach verify the authenticity and integrity of the binary cheque image, but also can locate the illegal modifications. The description of this proposed approach will be presented in the following section in details.

Methodology

This proposed combined approach is a kind of sender- receiver protocol, and it can be applied to exchange bank cheque electronically between the sender and the target receiver. The sender generates a binary image from the scanned color cheque image, extracts a content-dependent *AS* from the resultant binary image and embeds it back into the binary image again. This *AS* enables the recipient of the signed binary cheque image to authenticate its sender and to verify that the cheque is intact. Hence, in the receiver side, the authenticity and integrity of the cheque are verified by comparing the *AS* and watermark both extracted from the received binary cheque image, and the original cheque is recovered precisely. All the necessary processes and

steps, which involved in both the sender's and the receiver's sides, will be described below and depicted in block diagrams.

A. The Image Binarization:

Most of the image binarization procedures try to separate the foreground (objects) from the background. Hence, a simple and efficient way for binarization is converting the colored image into gray-scale image and then thresholding it. For that it is essential to choose good threshold level in order to produce a readable binary image. As shown in Fig.(1), this research suggests an image binarization procedure with a subjective threshold level evaluation being achieved by applying the spatial filters (like maximum and minimum filters). Let the original colored cheque image and the produced gray scale image are represented as *F* and *Gray*, respectively. The *Gray* can be produced by applying equation (1) as follows:

$$Gray_{(x,\,y)} = F_{(x,\,y)}\ \frac{r+g+b}{3} \quad \text{..... (1)}$$

Where *x* and *y* are the *x* and *y* axes for each pixels in image *F*. the values *r*, *g* and *b* are the red, green and blue color values for that pixel. $Gray_{(x,\,y)}$ is the resultant gray level value for that pixel. After that, 3×3 maximum and minimum filters, which select the largest and the smallest pixel value within 3×3 sliding over window of pixel values for each pixel in the *Gray*, are applied respectively. The resultant images are named as *MAX* and *MIN*. the threshold image *T*, which represents the threshold levels for all pixels in *Gray*, is produced by using relation (2). Then, the *Gray* is matched against *T* to produce the binary image *Binary*, by applying the relation (3).

$$T_{(x,\,y)} = \begin{cases} \frac{(MIN(x,y) + MAX(x,y))}{2} & \text{if } Gray_{(x,\,y)} \geq MIN_{(x,\,y)} \\ 0 & \text{otherwise} \end{cases} \quad \text{..... (2)}$$

$$Binary_{(x,\,y)} = \begin{cases} 1 & \text{if } Gray_{(x,\,y)} \geq T_{(x,\,y)} \\ 0 & \text{otherwise} \end{cases} \quad \text{..... (3)}$$

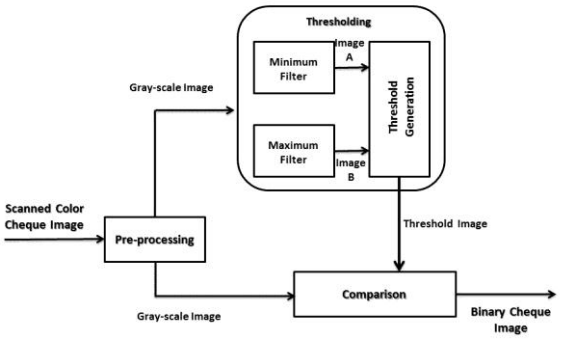

Fig. (1) The Binarization Process.

B. The Image Partitioning

The binary image, which is represented in the previous section as *Binary*, will be partitioned into (3×3) blocks. Each block will be checked against predefined 3×3 patterns. If a block matches with any of the valid patterns, it will be ready to hide the *AS*. And it will be referred as *Ready Block* whose middle pixel can be used to hide the *AS*. Hence, few pixels will be modified. And the positions of *Ready Blocks* containing those pixels will be detected in the insertion and extraction or detection processes. Furthermore, only low-visibility pixels can be used to hide *AS* and consequently the signed binary image will have good visual quality and non-modified image fingerprint. Fig.(2) shows the block patterns which are used to find ready blocks [4, 5]. The hatched middle pixel may either be black or white. The change of middle pixel is less noticeable. Mirrors, transposes and reverses of the patterns may also be used for hiding *AS*. Those predefined patterns are selected based on the following constraints:

a) The number of white pixels in a block must be greater than 2 and less than 6 excluding the middle pixel. That is, 3, 4, 5 or 6 white pixels and 6, 5, 4 or 3 black pixels respectively.
b) If there can be only 3 white/ black pixels, they must not be in the same row/column.

As shown in Fig.(3), once the *Ready Blocks* can be found, it will be clearly understood that the middle pixels of them will form the *ASR*. The *AS region* (or *ASR*) is the region where the *AS* will be embedded, and consequently it will be small in size. Whereas, the binary image excluding *ASR*, will be named as *Non-ASR* (or *NASR*) from where the

AS will be generated or computed, and it is larger in size.

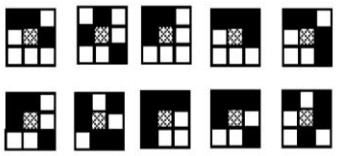

Fig. (2) The 3×3 block patterns used for data hiding. The hatched middle pixel may either black or white. The change of middle pixel is less noticeable. Mirrors, transposes and reverses of the above patterns are also used for date hiding.

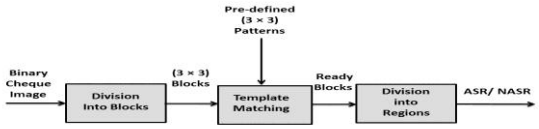

Figure (3) : The Partitioning Process.

Fig. (3) The partitioning process.

C. The *AS* Generation

The content based robust bits, which form *AS*, will be extracted from the binary image by using the method proposed in [8], but with an extended idea. Given *ASR* that contains *N* "middle pixels" of *N Ready Blocks*, and *NASR* that contains the other *K* pixels extracted from each *Ready Block* with the excluding of its middle pixel, forming a string of information whose length will be $k \times N$ bits or *Z* bits, i.e., $Z=k \times N$. Using a secret key, *Z* random matrices will be generated whose entries will be uniformly distributed in the interval [0, 1]. After excluding the middle pixels of each *Ready Block*, each *Ready Block* will be projected on its corresponding generated ***Z*** matrix to obtain a scalar value *v*. Then the absolute value of *v* will be compared with a threshold value ***t*** to obtain a bit named as *b* by using the relation (4). Then all the bits obtained from the ready blocks altogether, will form *AS* which needed to be inserted:

$$b_i = \begin{cases} 0 & \text{if } |v_i| < t \\ 1 & \text{if } |v_i| \geq t \end{cases} \quad \text{.....(4)}$$

D. The *AS* Insertion (The Sender Side)

Once the cheque image is binarized and partitioned into *ASR* and *NASR*, and the *AS* is generated; the insertion of *AS* into the *ASR* of the binary cheque image is performed. The middle pixels that containing in the *Ready Blocks* and that form *ASR* are flipped to hide the bits or pixels of *AS* individually, i.e., each single pixel in *AS* is inserted into the center pixel of a *Ready Block*. Hence, the complexity of this proposed data hiding approach is not in identifying the position of those middle pixels (or *ASR*) but in identifying the *Ready Blocks* containing them. This complexity helps in providing another security level as well as that of the secret key. Fig.(4) shows the necessary steps which the insertion process involves at the sender side. And the following algorithm explains the whole insertion process.

Algorithm (1):

Let *Binary* be the binary cheque image to be signed and *Z* be the length of *AS* to be inserted:

1. Partition *Binary* and obtain *Z* (3×3) *Ready Blocks* to insert *Z* bits of *AS*.
2. The *ASR* can be computed from the middle pixels of *Z Ready Blocks*. *NASR* is obtained by excluding ASR from *Ready Blocks*.
3. Given *NASR* and a ***secret key***. Generate *AS* by using relation (4).
4. Insert *AS* into *ASR*.

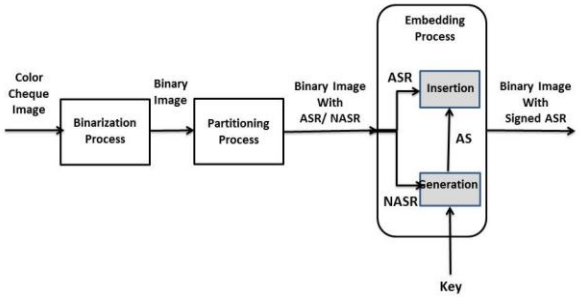

Fig. (4) The Embedding Process at the Sender Side.

E. The Detection of *AS* (The Receiver Side)

In the receiver side, as shown in Fig.(5), given the secret key, the same blocks – based method is performed to extract the *AS* from *ASR* and compute the *ID watermark* from *NASR*. Then the extracted *AS* is compared with the *ID watermark*. If they are not matched then the received binary cheque image is regarded as being modified by others. The following algorithm explains the whole detection process.

Algorithm (2):

Let *Binary** be the signed binary cheque image received.

1. Partition *Binary** and obtain *ASR* and *NASR*.

2.Extract *AS* from *ASR*.
3.Given *NASR* and the ***secret key*** generate *ID watermark*.
4.Match the *ID watermark* with *AS*. If they match then the received binary cheque image is authentic. Otherwise, it is not.

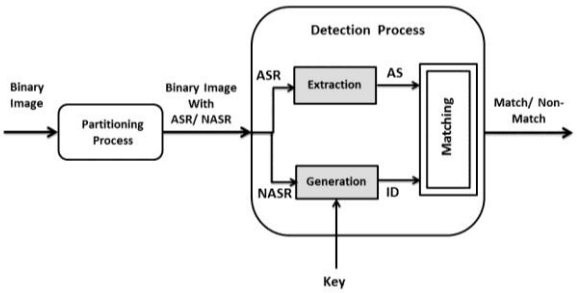

Fig. (5) The Detection Process at the Receiver Side.

Experimental Results and Discussion

In this section, experimental results are illustrated to demonstrate the validity of the suggested data hiding approach. A cheque image is taken as a sample image in the experiment whose results are showed in Figs. (6) and (7). Fig.(6) shows the results of the binarization process. Fig.(7) shows the results of detection process as follows: the original binary cheque image, the watermarked binary cheque image with the embedded *AS*, and the difference between the watermarked and original binary cheque image. By observing the watermarked binary cheque image, it is clear that the visual quality generated by this proposed blocks-matching based data hiding approach is good.

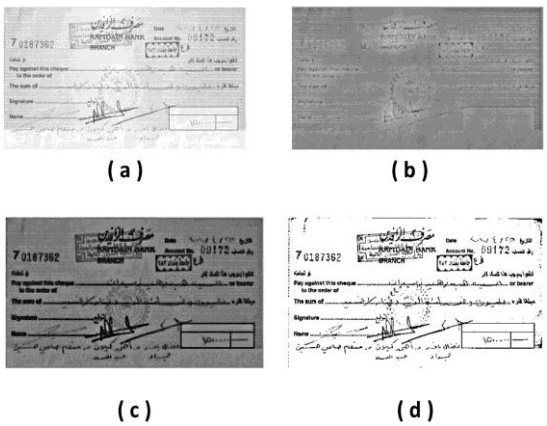

Fig.(6) The results of the binarization process, (a) the original gray scale cheque image, (b) the result of minimum filter application, (c) the result after applying the maximum filter, and (d) the resultant binary cheque image.

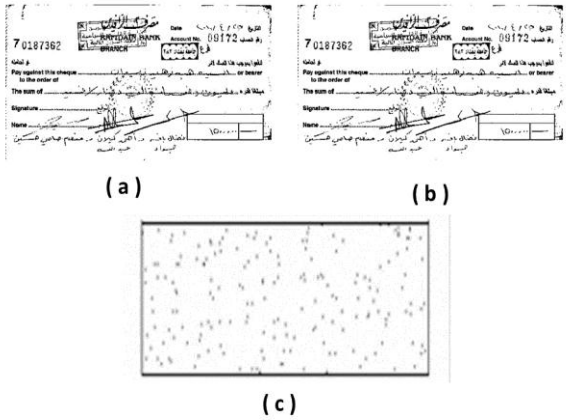

Fig.(7) The results after applying embedding and detection algorithms, (a) the host binary cheque image, (b) the watermarked binary cheque image with AS, and (c) the difference between (a) and (b) shown in black points.

Two mathematical metrics are used to compare the original binary cheque image against the marked binary cheque image with AS, the *mean square error* (*MSE*) and peak signal to noise ratio (PSNR)**.** The *MSE* is the accumulative squared error between the two compared images and the *PSNR* measures the objective difference between the two compared images [4]. The mathematical formula for *MSE* and *PSNR* are as follows:

$$MSE = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\frac{(I(x,y)-I''(x,y))^2}{M\times N} \quad \text{..... (5)}$$

$$PSNR = 20\times log_{10}\frac{255}{2\sqrt{MSE}} \quad \text{..... (6)}$$

Where *I(x, y)* is the original binary cheque image (the host image) and *I''(x, y)* is the watermarked binary cheque image with *AS*, and *M, N* are the dimensions of the two compared images. A lower value for *MSE* means less error, and as seen from the equation (6) this reveals the higher value for *PSNR*. If the watermarked binary cheque image has a lower *MSE* and a high *PSNR*, it is referred to a better result because *PSNR* means that the ratio of signal (it is the original binary cheque image) to noise (it is the modified pixels for the binary cheque image after the embedding of *AS*). The sample cheque image reveals the experimental results for this proposed approach as follows: the image size in bits 252×282, the number of 3×3 sub-blocks

is 7896, the number of ready blocks is 330, the number of modified pixels is 89, the *MSE* is 0.0015, and the *PSNR* is 29.023.

Conclusions

This research has proposed a secure model for the electronic transfer of typical bank cheque as a substitution of the physical paper-based bank cheque exchange between the depositing and the paying banks. This proposed model involves representing the typical bank cheque in a simple digital format –i.e. binary image- because binary images bring great memory saving and legibility. Hence, the textual parts that the cheque contains can be preserved legible without halos around the border of the text. Also, the saving of much storage by using binary image will lead to band reduction during the electronic transmission. Furthermore, a blocks-based data hiding is proposed for binary cheque image to protect the binary version of cheque image against alteration and fraud. An authentication signature is extracted and embedded from and to a part of the binary cheque image itself, without changing the image's visual quality. The good performance is shown by the experimental results which demonstrate that the proposed model can be suitable for signing digitally the binary cheque image without causing noticeable loss of its quality and for securing the binary versions of bank cheque image during its transmission through the open computer networks like Internet.

References

[1] M. Younes, A. Jantan, "A New Steganography Approach for Image Encryption Exchange by Using The Least Significant Bit Insertion", IJCSNS International Journal of Computer Science & Network Security, vol. 8, No. 6, June 2008.

[2] S. D. Pamboukian, H. Y. Kim, R. L. De Queiroz, "Watermarking JBIG Text Region For Image Authentication", 0-7803-9134-9/05/2005, IEEE.

[3] H. Y. Kim, R. L. de Queiroz, "A Public key Authentication Watermarking For Binary Images", School of Polytechnics, University of Sao Paulo, Brazil, IEEE, 2004.

[4] M. Venkatesan, P. Meenakshidevi, K. Duraiswamy, "Secure Authentication Watermarking for Binary Images Using Pattern Matching", IJCSNS International Journal of Computer Science and Network Security, vol. 8, No. 2, February 2008.

[5] H. Y. Kim, A. Afif, "Secure Authentication Watermarking for Binary Images", in Proc. Sibgrapi-Brazilian Symp. On Computer Graphics & Image Processing, pp. 199-206, 2003.

[6] H. Y. Kim, A. Afif, "Secure Authentication Watermarking for Halftone & Binary Images", Int. J. Imaging Systems & Technology, vol. 14, No. 4, pp. 147-152, 2004.

[7] Min Wu, member IEEE and Bede Liu, fellow IEEE, "Data Hiding in Binary Image for Authentication and Annotation", IEEE Transactions on Multimedia, vol. 6, No. 4, August 2004.

[8] D. Dias & R. De Queiroz, "A model for the Electronic Representation of Bank Checks", Brasilia University, 1-4244-0481, 9/06/2006, IEEE.

[9] I. J. Cox, M. L. Miller and J. A. Bloom, "Watermarking Applications & Their Properties", Int. Conf. On Information Technology, Las Vegas, 2000.

[10] E. Koch and J. Zhao, "Embedding Robust labels into Images for Copyright protection", in Proc. Int. Congr. Intellectual Property Rights for Specialized Information, Knowledge & New Technologies, 1995.

[11] Ch. Tsai, H. Chiang, K. Fan and Ch. Chung, "Reversible Data Hiding and Losseless Reconstruction of Binary Images mechanism", Pattern recognition, vol. 38, issue 2, November 2005.

[12] M. Venkatesan, P. Meenakshidevi, K. Duraiswamy, "A New Data Hiding Scheme with Quality Control for Binary Images Using Block Parity", Information Assurance and Security, IAS Manchester, UK, pp. 468-471, 2007.

المصرفي الذي يمكن ان نطلق عليه تسمية (الصك الالكتروني) بين المؤسسات المصرفية عبر الانترنيت.

الخلاصة

نقترح هذا البحث، مزيجا من أسلوبين هما التمثيل و التوثيق الرقمي للصك المصرفي المتبادل الكترونيا بين المصارف او البنوك عبر شبكات الحاسوب المفتوحة و غير الآمنة مثل شبكة الانترنيت و ياتي ذلك عوضا عن التبادل المعتاد للصك المصرفي بصيغته الورقية. و يمكن ان يعد هذا المزيج المقترح بروتوكولا بين المرسل– المستلم. حيث يقوم المرسل بإجراء مسح ضوئي ملون بسيط للصك المصرفي الورقي ليتم خزنه بهيئة صورة رقمية ملونة يتم تحويلها الى صورة ثنائية اللون (ابيض– اسود) و يتم عمل توقيع رقمي مستخلص من بيانات الصورة و باستخدام مفتاح سري لغرض استخدامه لتوثيق الصورة من قبل المرسل. و بعد ارسال الصورة عبر الانترنيت الى الجهة المستفيدة (اي المستلم) سيتم التحقق من اصالتها من قبل المستلم وذلك باستخلاص التوقيع الرقمي مرة اخرى و باستخدام المفتاح السري سيتم برهنة سلامة الصورة من اي تغييرات غير مرغوب بها يمكن ان تتم اثناء عملية ارسال الصورة و تبادلها عبر شبكة الانترنيت يمكن ان يقوم بها اي مخترق او متطفل مستخدم لشبكة الانترنيت اثناء عملية التبادل الالكتروني للصك المصرفي. كما ان عملية استخلاص و اخفاء او بناء التوقيع التوثيقي الرقمي في صورة الصك الثنائية يتم بتقسيم الصورة ذاتها الى مقاطع صغيرة الحجم و قليلة الابعاد بحيث يمكن الاستفادة منها في تحديد محل و موقع اي تغيير يمكن ان يتم على الصورة الثنائية المضيفة. و قد تم اجراء تجربة عملية على بعض الصور الثنائية لنماذج من الصكوك المصرفية و باستخدام بعض المعايير و المقاييس الرياضية تم اختبار صحة و فعالية اسلوب استخلاص و اخفاء البيانات من الصور الثنائية المقترح في هذا البحث... و قد بينت نتائجها بان هذا المزج من اسلوبي التمثيل الرقمي و اخفاء البيانات المستخلصة من صورة الصك ذاتها.. يمكن استخدامه لاجراء توقيع توثيقي رقمي للصكوك المصرفية التي يتم تمثيلها و تبادلها الكترونيا غبر شبكة الانترنيت دون حدوث اي تأثير ملحوظ على صورة الصك الرقمية و جودتها... كما ان هذا الاسلوب المقترح سيساهم في توفير اكبر سعة خزن و موجات نقل ممكنة اثناء عملية التبادل الالكتروني للصك