International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.3, Issue.1, Jan-Feb. 2013 pp-354-359 ISSN: 2249-6645

A Survey on Authentication for Grayscale Images Based On Visual Cryptographic Technique

B. Priyanka[1], E. Purushottam, [2]

Abstract: *A new digital watermarking technique as authentication method based on secret sharing sharing method for color images was proposed. The image is transformed in to binarized block form in which the watermark is embedded for authentication purpose and then the image is divided into several shares using shamir secret sharing scheme, which reconstructs the secret by using reverse Shamir secret sharing scheme and is been proceeded for authentication process i.e to check the watermark embedded in the image.*

Key Words: *digital watermarking, secret, Shamir secret sharing, image authentication.*

I. NTRODUCTION

Digital information is a form of preserving data for which authentication is necessary to overcome the tampering attacks. In multimedia applications, it is necessary to authenticate the source image which might be subjected to tampering. So, for such content authentication watermarking technique is used. It is one among the emerging fields that are used for content authentication. As, the content authentication is being the hottest topics now a days, it is necessary to assure that the delivering of image to somewhere is delivered as it is. However, with the fast advance of digital technologies it is easy to make the modifications to the images. Thus integrity of image become a serious concern. To solve those image authentication problem particularly digitized documents, digital signatures, tables, texts, etc., whose security must be protected. In this paper we are performing image authentication of grayscale images. Grayscale image has two gray values i.e foreground and background. Grayscale images look like binary ones. So, we can call a grayscale image as binary like grayscale image. Binary image consists of two colors black and white. Using binary images can cause some problems. As the binary images are simple in nature many unpleasant strokes can encounters. So using grayscale images can solve the problem of visual quality which the binary one cannot does.

Many conventional methods have been proposed for authentication of grayscale images. In our proposed method, the image is first watermarked and divided into shares using Shamir secret sharing scheme. Later, those shares are reconstructed using inverse Shamir secret sharing scheme and watermark has been extracted if the image is authentic. Data loss during transmission are marked as gray blocks.

Grayscale cheque image

II. DIGITAL WATERMARKING

Digital watermarking is a technique for inserting a watermark into an image, which is been later extracted or detected for identification and authentication purposes. A watermark is a form of text or image that is been embedded in to the paper for its evidence of authenticity. The extension of this concept is Digital watermarking. Watermarks are of two kinds: visible and invisible. It is related to steganography but, in watermarking technique the information that is hidden is usually related to the cover object. It is used for content authentication and copyright protection.

Digital watermarking is defined as the digital signal that is embedded in audio, video or image with some information related to those and which cannot be eliminated easily.

The process to embed a watermark is done in three steps:

1. ***Embedding watermark***: In this algorithm it accepts the data to be embedded and produces watermark signal.

2. ***Attack on image***: The watermark signal is transmitted and during transformation the attacker may or may not modify the image. If there is a modification then it is said to be an attack.

3. ***Detection of watermark***: This algorithm is applied when the attacked signal to extract watermark from it. If the signal undergoes any modification then the information is also carried in the copy. If suppose, the signal doesn't undergo any modification the watermark is present and it can be extracted.

We first embed the watermark in to the original or cover image and make it a watermarked image and then after transformation we extract the watermark and check whether it has been undergone any sort of manipulations or attacks. Finally, we extract the watermark from the image to prove its authenticity. To avoid illegal access to the watermark a secret key as shown in the figure is used during the embedding process and extraction process of watermark.

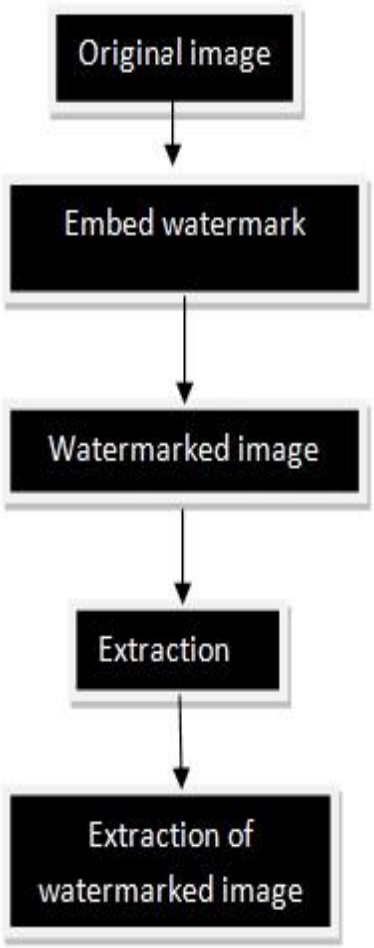
Watermarking techniques are used for copyright protection, broadcast monitoring, authentication, tamper detection and digital finger printing, content protection, content labeling.

A watermark may be:

1.Robust: As the names mentioned it is strong and overcomes sevreal processing attacks. For example: filtering, compression

2.Fragile: It is distorted under slight changes.

3.Semi-fragile: It breaks under the changes performed by the user i.e exceeding specific threshold.



Block diagram of watermarking

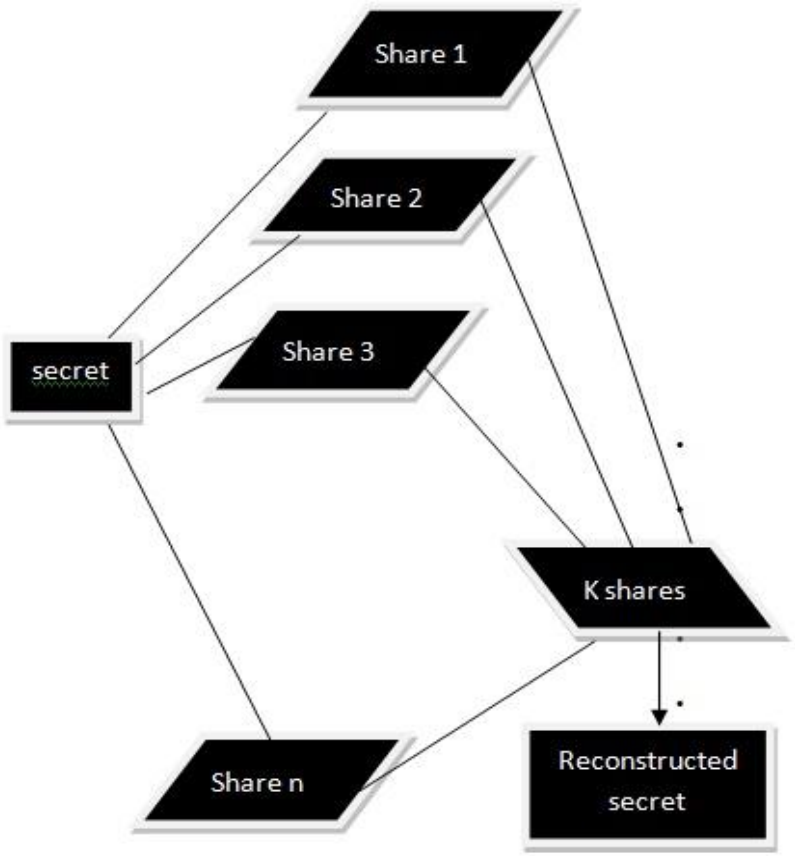
III. SECRET SHARING METHOD

During decades some scientists (eleven) are working on a secret project. They wish to lock up the documents and details of the secret project in a cabinet so that the cabinet can be opened if and only if six or more of the scientists are present. So, What is the smallest number of locks needed to open the documents? What is the smallest number of keys to the locks each scientist must carry to view the documents?

The method of secret sharing is sharing a secret among group of participants. It is come to know that previously there are some eleven scientists who are working on a secret project for which they wanted to lockup their documents regarding the project with some secret code. So there the problem arises. They want those documents to be enclosed to the cabinet only if six or more scientists opens it with their individual secret key share. It means cabinet consisting of eleven members having their own individual unique secret key. But in order to access the documents of project a single secret share key not sufficient and at the same time it is not necessary to have all eleven secret share keys to open the documents. So for this Shamir proposed an algorithm named Shamir secret sharing algorithm where a single secret is shared among group of participants. Here participants are the authorized users who access to the data.
The algorithm goes in the following manner:

1. Divide the data d in to n pieces i.e d1, d2, d3, d4,…….dn
2. It is distributed among n participants.
3. The secret or data can be reconstruct able only if k pieces are present.
4. Even k-1 pieces are not acceptable.

So he proposed a scheme called (k,n) threshold scheme. Where k is the minimal number of users or participants to reconstruct the key and n is the total number of divided pieces of data or secret. For example: a company wants to sign the checks by the executives in a digitized manner. At the same time company's signature must be secret, so the if we give the company's signature to all the executives then it is pruned to privacy attacks. So in order to solve this problem they are using (k,n) threshold scheme i.e they are putting a minimal number of key as 3 i.e (3,n) they are given a magnetic card with that. The company president is given 3 keys, vice president is given 2 keys and the executive is given a single one. So in order to prune to any attacks the executive must have still 2 keys and the vice president must have still one more key.



Secret sharing method

IV. PROPOSED METHOD

Original image is authenticated by embedding a watermark which is invisible. Later, the image is divided into shares using Shamir secret sharing method and the divided shares are transferred and by using inverse Shamir secret sharing method we form the original image and the watermark is extracted from that image to authenticate.

Embedding watermark: An image A is selected form set of standard images and let it be the base image on which a watermark is embedded.

Algorithm:
Step 1: Let *B* be a grayscale image to be watermarked.
Step 2: Use a pseudo-random number generator with a known seed to generate a set of non repeating pseudo-random locations *L* within the grayscale image *B*.
Step 3: Clear all pixels of *B* that belong to *L*, obtaining *B**.
Step 4: Compute the fingerprint *H* .*H*(*B**).
Step 5: perform exclusive-or *H* for getting the marked fingerprint H^*.
Step 6: Encrypt *H** with the secret key or private key thus generating the MAC/DS *S*.
step 7: Insert *S* into the set of pixels *L*, generating the watermarked image *B*

Diving the shares: We apply (k,n) threshold secret scheme for dividing the watermark image into shares. The following is the algorithm for dividing the watermark image in to shares.

Algorithm:

Step 1*: Take secret d in the form of an integer, number n of participants, and threshold k<=n.*
Step 2*: Choose a random prime number p larger than d.*
Step 3*: Select k-1integer values* $c_1,c_2,c_3,\ldots\ldots$ $\ldots,c_{k-1}$ *range of 0 through p-1 .*
Step 4*: Select n distinct real values* $x_1,x_2,x_3\ldots\ldots$ $\ldots\ldots,x_n$
Step 5*: Use the following (k-1) degree polynomial to compute n function values* $F(x_i)$ *, called partial shares for i=1,2,….n i.e*

$$F(x_i) = \left(d + c_1 x_i + c_2 {x_i}^2 + \cdots\ c_{k-1} {x_i}^{k-1}\ \right) mod\ p$$

Step 6*: Deliver the two-tuple* $(x_i,F(x_i))$ *as a share to the i participant where i=1,2,3,…n .*

Reconstructing the shares: We reconstruct the shares by applying inverse Shamir secret sharing scheme. The following is the algorithm reconstructing the watermarked image.

Algorithm *:*

Step 1*: k shares collected from the n participants and the prime number p with both k and p*
Step 2*: Use the k shares* $(x_1,F(x_1)),(x_2,F(x_2)),\ldots,(x_k,F(x_k))$ *to* $F(x_j) = \left(d + c_1 + c_2 {x_j}^2 + \cdots + c_{k-1} {x_j}^{k-1}\right) mod\ p$ *where j=1,2,….k*

Step 3*: Solve the k equations above by Lagrange's interpolation to obtain d as follows*

$$d = (-1)^{k-1}[F(x_1)\frac{x_2 x_3 \ldots x_k}{x_1 - x_2)(x_1 - x_3)\ldots(x_1 - x_k)}$$

$$+F(x_2)\frac{x_1 x_3 \ldots x_k}{(x_2 - x_1)(x_2 - x_3)\ldots(x_2 - x_k)} + \cdots$$

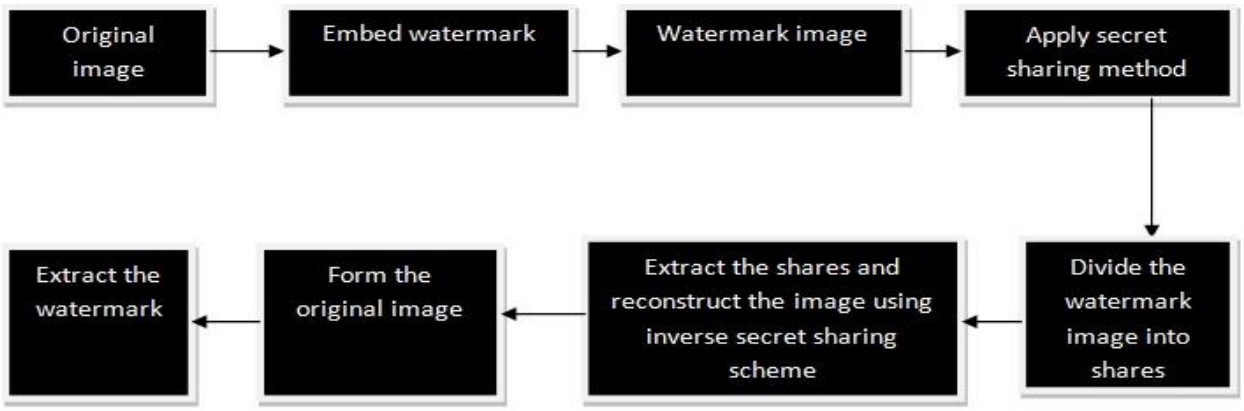
$$+F(x_k)\frac{x_1 x_2 \ldots x_{k-1}}{(x_k - x_1)(x_k - x_2)\ldots(x_k - x_{k-1})}]\ mod\ p$$

Step4*: Compute* c_1 *through* c_{k-1} *by expanding the following equality and comparing the result with Step 2 while regarding variable x in the equality below to be* x_j

$$F(x) = [F(x_1)\frac{(x - x_2)(x - x_3)\ldots(x - x_k)}{(x_1 - x_2)(x_1 - x_3)\ldots(x_1 - x_k)}$$

$$+F(x_2)\frac{(x - x_1)(x - x_3)\ldots(x - x_k)}{(x_2 - x_1)(x_2 - x_3)\ldots(x_2 - x_k)} + \cdots$$

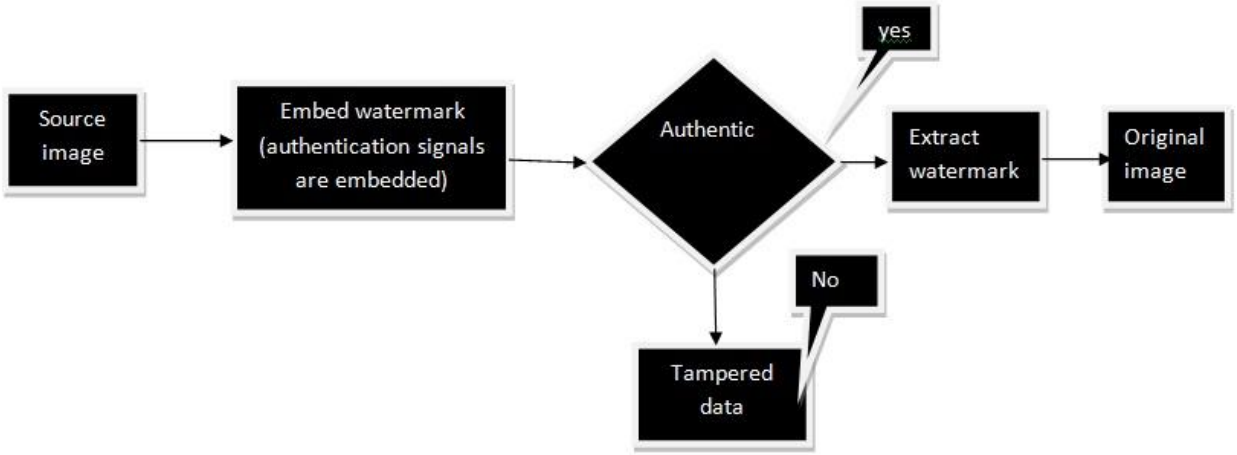
$$+F(x_k)\frac{(x - x_1)(x - x_2)\ldots(x - x_{k-1})}{(x_k - x_1)(x_k - x_2)\ldots(x_k - x_{k-1})}]\ modp$$



Process for authentication of grayscale cheque image

Extraction of watermark:

Algorithm:
Step 1: Let *X* be a watermarked image. Use the same pseudorandom number that has been applied in insertion process to generate again the same set of non repeating pseudo-random locations *L* where the watermark has been inserted.
Step 2: Let *X** be the image obtained from *X* by clearing all pixels in *L*. Using the same hashing function *H* compute the fingerprint *H* .*H*(*X**).
Step 3: Extract the watermark from *X* by scanning pixels in *L* and decrypt the result using the secret key and obtain the decrypted data D.
Step 4: By applying exclusive-or *H* with *D*, obtaining the check image *C*.
Step 5: If *C* and *A* are equal, the watermark is verified. Otherwise, the image *X* has been modified. The following is the procedure for authentication.



V. EXPERIMENTAL RESULTS

The following are the experimental results performed on grayscale cheque image. A cover image is taken and performed the authentication process. Firstly, embed a water in to the image by using algorithm 1.

(a)

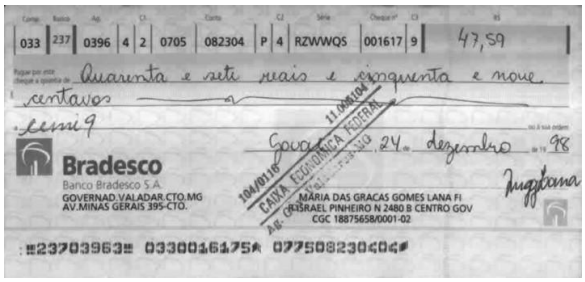
(b)

Experimental results for cheque image (a) cover image or original image (b) embedded watermark image

Later, the image is divided in to shares using Shamir secret sharing method. The shares are reconstructed using inverse Shamir secret sharing scheme and form a original or cover image. Then, check for the watermark embedded in the image. The image is said to be authentic if watermark is present. Extract the watermark. There occurs, a loss of data during the transmission process, which is marked as gray blocks as shown in the figure. If there is no data loss during transmission the original image is recovered.

The following are the figures related to the image with tampering i.e the tampering is shown in the form of gray blocks and without tampering i.e original or cover image.

(c)



(d)

(c) Image with tampering shown in the form of gray blocks (d) original or cover image without tampering.

VI. CONCLUSION

In, this paper a new image authentication using secret sharing method is proposed. The grayscale cheque image is watermarked first and that watermark is divided in to shares using Shamir secret sharing method. Later, the shares are reconstructed using inverse Shamir secret sharing scheme and the watermark is extracted. Data loss during the transmission is shown in the form of gray blocks. This can be performed for color images also.