ISSN 2047-3338

Visual Cryptography Authentication for Data Matrix Codes

M. Agnihotra Sharma[1] and M. Chinna Rao[2]

***Abstract*— An Identity Card is any document which may be used to verify aspects of a identity. If issued in the form of a small, mostly standard-sized card, it is usually called an identity card (IC). It plays in the society, threats of fraud, tampering, and identity theft arises. Thus, security and authenticity of these ID cards and their owners prove to be of much necessity. This paper goal is to make use of Visual Cryptography and 2D data matrix codes to address these issues. Visual Cryptography is a secret sharing scheme where a confidential image is encrypted into noise-like secure shares, which can be reconstructed visually by superimposing the shares. Extended Visual Cryptography on the other hand, makes use of recognizable images as shares to the confidential image. In this paper, the information in the ID cards are encoded into two 2D data matrix codes, which then are used in the two levels of extended visual cryptography. The first level provides authentication of the ID card, and the second level secures the identity of the ID card owner.**

***Index Terms*— Visual Cryptography, Extended Visual Cryptography, 2D Data Matrix Code, Data Matrix Code, Seed Image and Share Image**

I. INTRODUCTION

IDENTITY Cards or ID cards play vital role in the society. An ID card is used mainly to verify a person's identity, and most of them contain private information such as addresses, contact numbers, and the like. With its underlying significance, the threat of fraud arises and thus the need for securing the authenticity of such documents. Also, for safety and privacy, ID card owners may want to secure the private information contained in these documents, such as the credit card number in a credit card, the student number in a school ID, and maybe even the address, contact number, and the picture of the owner.

To address the issue of authenticity and security of the owners, the use of two-dimensional data matrix codes and biometric identifiers in machine-readable cards is introduced. A two-dimensional data matrix code or 2D data matrix code, similar to a linear data matrix code, is an optical, machine-readable representation of data which uses the vertical dimension to compactly store and retrieve more information.

Nowadays, in ID card applications a 2D data matrix code symbol contains the person's personal information and is present in the ID card to prevent tampering and identity theft.

A biometric identifier is an objective measurement of a physical characteristic of an individual which can be used to verify the person's identity. It exists in many forms such as fingerprint, facial image, and iris template. In many applications, biometric identifiers may be embedded in different ways. One method is visual cryptography.

Visual cryptography is a secret sharing scheme where a secret image is encrypted into shares, which are noise-like secure images that can be distributed over an untrusted environment. The secret image can be reconstructed visually by superimposing the shares. This scheme can be extended such that recognizable images are used as shares and still retain the property of yielding the final image when superimposed. The advantage of visual cryptography is that it can be used to address both the issues on privacy and security. An image may be kept hidden through the secret sharing scheme, and at the same time it is secured as well as its shares.

This project aims to secure the authenticity of ID cards as well as the private information stored in them. In authenticating the ID card, two aspects are checked: the ID card's membership to the system or organization which addresses the concern to whether or not the ID is a fake; and the person's ownership of the ID card, which addresses the concern to whether or not an ID card truly belongs to a person. Two 2D data matrix code symbols are stored in an ID card: one contains the "public" information - those that can be disclosed to the public - and the other contains the private information. The first data matrix code is readily read by a 2D data matrix code decoder. The public information is stored in a data matrix code for machine readability - with this, digital logging and recording of information from the ID card is easier. The second data matrix code contains the encrypted private information, which can only be read with a password or a key after decoding using a decoder. Two levels of extended visual cryptography are implemented. In the first level, the public data matrix code and a master seal, not known to the owner, are used as the shares of a master data matrix code, which contains a key for authenticity, also not known to the user. In the second level, the two data matrix codes are used as the shares of the facial image of the owner. Through this, the identity of the owner is secured as the facial image will only be displayed upon superimposing the two data matrix

M. Agnihotra Sharma with the Kakinada Institute of Engineering and Technology, Kakinada, Andhra Pradesh, India, (Corresponding author: phone: 9491520200; e-mail: agni2020@ gmail.com).

M. Chinna Rao, Associate Prof. with the Kakinada Institute of Engineering and Technology, Kakinada, Andhra Pradesh, India, (e-mail: chinnarao.mortha@gmail.com).

codes. Also, with the facial image encrypted on the data matrix code shares, faking the ownership of an ID card by simply replacing the face image or even changing the printed information on the ID is prevented. The authenticity is also secured, as the public data matrix code must match the master seal for it to yield a master data matrix code with a valid key upon decoding

II. TWO-DIMENSIONAL DATA MATRIX CODE TECHNOLOGY

Two-dimensional data matrix codes or 2D data matrix codes are optical, machine-readable representation of data. Unlike the linear data matrix code, 2D data matrix codes make use of the vertical dimension to pack in more data.

Over 20 2D data matrix code technologies are now available, the most popular of which are the symbol, QR code, and data matrix. In this paper, the data matrix code is used, and the following subsection describes its structure which makes it suitable for this project.

A. Architecture of the Data Matrix Code

Barcode is a stacked linear bar code symbol format used in a variety of applications, primarily transport, identification cards, and inventory management. PDF stands for Portable Data File. An example of the symbol is shown in Fig. 1, together with its parts, if a barcode symbol consists of three to ninety rows of data matrix coded information. As seen in Fig. 1, each row has a quiet zone, a start pattern, row indicators, a data region, and finally a stop pattern. The data region for each row may contain one to thirty code words.

Codeword is the encoded representation of a value between 0 to 928. It consists of four bars and four spaces. A bar or space may vary in width from one to six modules but the total module length of a single codeword will always be 17.makes use of Reed Solomon error correction. This error correction allows the symbol to endure some damage without causing loss of data. The level of error correction is user defined and ranges from 0 to 8. The number of code words that can be corrected are equal to (2^k+1)-2, where k is the error correction level. This means, for example, at level 6, up to 126 code words can be corrected.

Compared to other data matrix codes, provides greater levels of error correction. This makes it more suitable for the Visual Cryptography scheme as it often results in heavily noised images.

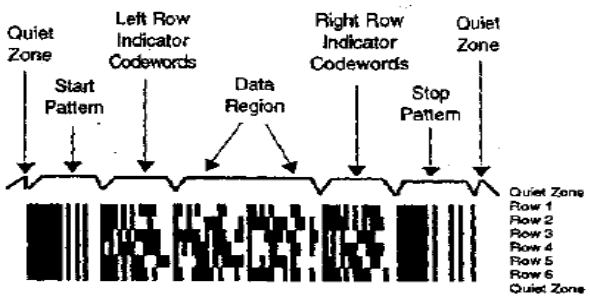

Figure 1: Data matrix and its parts

III. VISUAL CRYPTOGRAPHY SCHEME

Visual Cryptography (VC) is a cryptographic technique which allows visual information to be encrypted into several shares, each of which does not reveal any information on the confidential image. The confidential image is then easily decrypted by superimposing the shares.

A. Visual Cryptography Algorithm

In Visual Cryptography, the secret image contains two levels of illumination: a bright illumination with level 0.5 and a dark illumination with level 0. The shares to the secret image are constructed using this scheme: if the shares are the same then a bright illumination is shown; otherwise if they are complementary, a dark illumination will be shown. An example is shown in Fig. 2.

B. Extended Visual Cryptography Algorithm

Visual cryptography can be extended such that recognizable images are used as shares to the confidential image, and not only noise-like shares. There are various ways of implementing the extended visual cryptography. In this paper, the visual cryptography algorithm is extended by adding a third illumination, the gray illumination. For the shares, the levels of illumination are from 0.75 to 0.25, while for the secret image the levels of illumination range from 0.5 to 0. The input images which are used as shares, are modified using the secret sharing scheme, and from here the shares are generated using the respective levels of illumination. To minimize the error on the shares and on the result image, the calculation errors are distributed among the shares and the result image, Fig. 3 illustrates this scheme.

IV. EXTENDED VISUAL CRYPTOGRAPHY ON 2D DATA MATRIX CODES

A user's public and private information will be encoded into two separate data matrix codes. These data matrix codes will be referred to as "public data matrix code" and "private data matrix code" respectively. Before applying the method of visual cryptography on the 2D data matrix codes, both the set of seals and the set of master data matrix codes must first be generated. Seals are random noised images used as constant shares; i.e, it is not modified by the VC scheme since it is used in several sets of public and master data matrix code combinations for different ID cards. Master data matrix codes contain keys which are used to verify whether a data matrix code combination (the public and private data matrix code combination) is authentic or not.

A. Encoding Process

The visual cryptography method is applied in two levels. The first level secures the authenticity of the data matrix code combinations, and the second level secures the identity of the owner by encrypting his/her facial image. The following subsections describe in detail the procedures done in these levels, and Fig. 4 shows the diagram of the processes.

First Level: The public data matrix code and one of the seals are used as shares to the confidential image which is the master data matrix code. Both the seal and the master data matrix code are known only to the system. Since the seal is constant, the public data matrix code and the master data matrix code are the two which are modified, such that superimposing the public data matrix code and the seal produces the master data matrix code.

The master data matrix code that is then obtained from the two shares are decoded using a 2D data matrix code decoder. The decoded key from the master data matrix code is then used to verify the authenticity of the data matrix code combination and the ID card containing it as a whole. If the data matrix code combination is a fake, no master data matrix code will be obtained from this level, and furthermore no key will be decoded.

Second Level: In this level the public and the private data matrix code are used as shares to the facial image. This time, the public data matrix code is constant, since it has already been pre-calculated from the first level. It cannot be modified; otherwise it will not match the seal to produce the master data matrix code. The private data matrix code and the facial image are modified in this level such that superimposing the public and private data matrix codes produces the facial image. Since the shares do not reveal any information on the confidential image, the identity of the owner is secured as his/her picture is kept in the two data matrix codes.

B. Decoding Process

The encrypted images, i.e., the facial image and the master data matrix code, are decoded by simply superimposing their corresponding shares. Fig. 5 illustrates this process. The 2D data matrix codes on the other hand are decoded using a 2D data matrix code decoder. The public data matrix code and the master data matrix code are decoded directly, but the private data matrix code produces an encrypted data upon decoding. The key or password from the user is required to obtain the private information. However, since the data matrix code images produced in the visual cryptography scheme are oftentimes heavily noised, there is a large possibility that decoding the data matrix codes directly may result to some data loss. To resolve this, the data matrix code images are first restored to reduce possible errors before decoding. Restoring the image may include demising, applying averaging filters, etc.

Information can now be encoded into and decoded from data matrix codes. The private information is encrypted using a key with XOR encryption before encoding into a data matrix code. The data obtained by decoding the private data matrix code is decrypted using the same key.

Currently, the data matrix code shares can now be decoded using the data matrix codes after demising methods. Information decoded from the data matrix code prior to the application of the EVC method was consistent to the information decoded after the EVC method.

V. PROGRESS

An example of the two levels is shown in Fig. 6 and Fig. 7. Further testing of the two levels of the encoding process are currently being done to measure the overall efficiency of the method - from compatibility of shares and result images to data hiding and visibility. Different combinations of data matrix codes and most especially different types of face images are to be used for the experiments.

VI. GOAL

The goal of this project is to provide an alternative security on ID cards through the use of 2D data matrix codes and visual cryptography. Information are encoded in 2D data matrix codes which make them not readily available to anyone. The facial image is encrypted in the data matrix code images, preventing identity theft and providing security to the owners. Fake data matrix code combinations are detected in the first level of the method, thus providing authenticity and integrity to the ID cards.

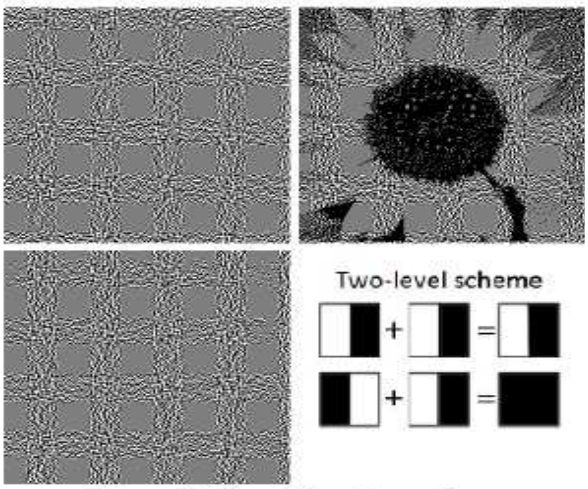

Figure 2. Visual Cryptography

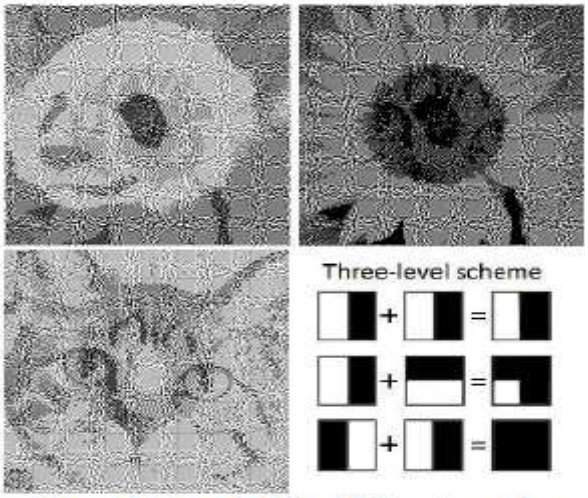

Figure 3. Extended Visual Cryptography

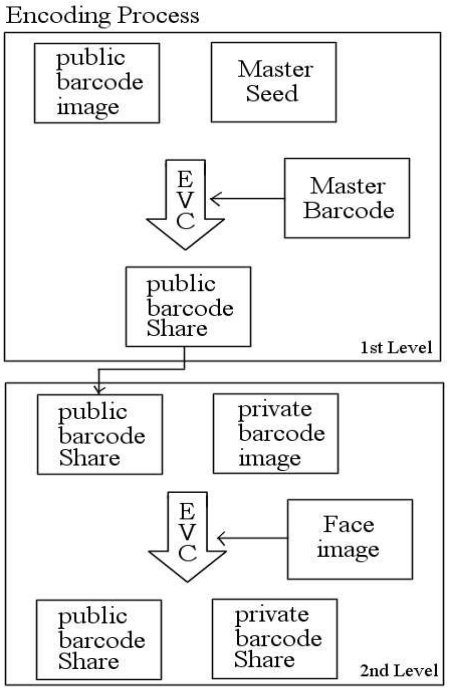

Figure 4. Encoding Process

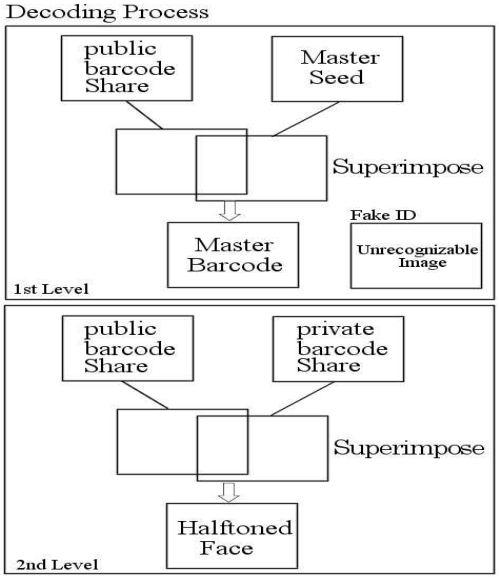

Figure 5. Decoding Process

REFERENCES

[1] Wang, Y.P., "System for Encoding and Decoding Data in Machine Readable Graphic Form" (September, 1993).

[2] Pei, S.C., and Guo, J.M., "Data Hiding in Halftone Images with Noise-Balanced Error Diffusion," IEEE Signal Processing Letters, Vol. 10, No. 12 (December 2003).

[3] Fu, M.S., and Au, O.C., "A Novel Method to Embed Watermark in Different Halftone Images: Data Hiding by Conjugate Error Diffusion (DHCED)," Hong Kong University of Science and Technology, Hong Kong, China (2003).

[4] Shen, J., "Progressive Halftoning by Perona-Malik Error Diffusion and Stochastic Flipping," University of Minnesota, Minneapolis, MN.

[5] Noore, A., Tungala, N., Houck, M., "Embedding Biometric Identifiers in 2D Data matrix codes for Improved Security," Computers and Security, 23, 679-686 (2004).

[6] Prakash, N.K., and Govindaraju, S., "Visual Secret Sharing Scheme for Color Images Using Halftoning," International Conference on Computational Intelligence and Multimedia

[7] Fu, M.S., Au, O.C., "Watermarking Technique for Color Halftone Images," Hong Kong University of Science and Technology, Hong Kong, China (2004).

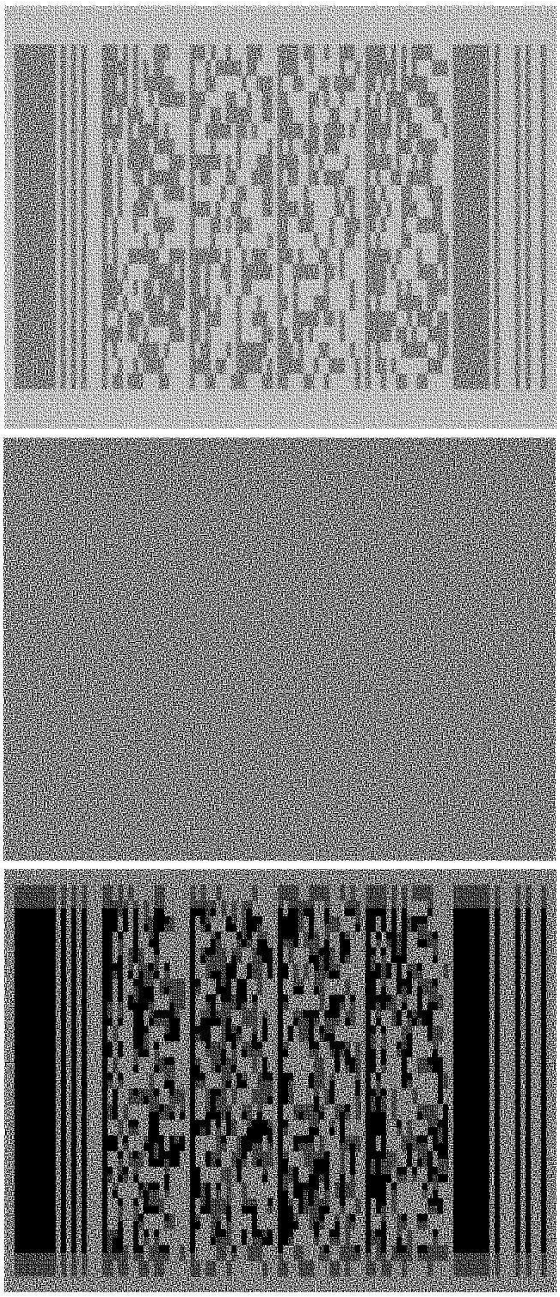

Figure 6. EVC Level 1

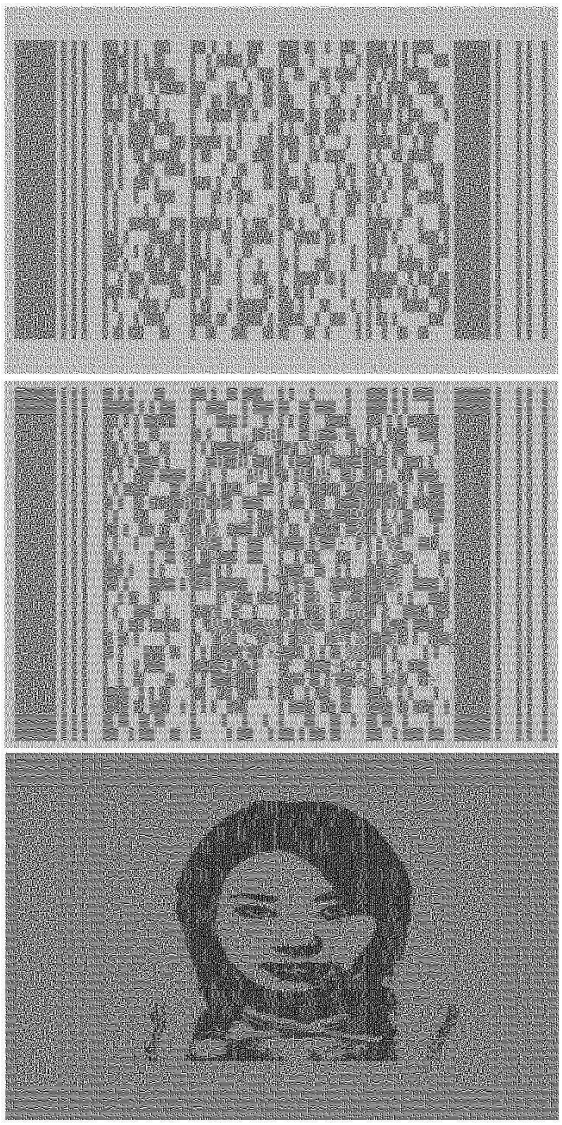

Figure 7. EVC Level 2

Agnihotra Sharma Munagala received the B. Tech degree in Computer Science and Engineering from Aditya Engineering College affiliated to JNTU, Kakinada, Andhra Pradesh, India in 2008. Presently,He is pursing M. Tech. in KIET, Kakinada, Affiliated to JNTUK, Kakinada, Andhra Pradesh, India. His research interests are Image Processing and Information Security.

Mortha Chinna Rao received the B. Tech degree in Computer Science and Engineering from JNTU, Hyderabad, Andhra Pradesh, India, in 2004, and also, received M.Tech, in Software Engineering from JNTU, Hyderabad, Andhra Pradesh, India, in 2008. Presently He is puring PhD in JNTUK, Kakinada, Andhra Pradesh, India. He is working as Associate Professor in KIET, Kakinada. His research interests include Data Mining and Emotion Recognition and Speech Recognition in Image Processing. He is member of Computer Society of India and Indian Society for Technical Education.