Volume 6, Issue 6, June 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Extended Visual Cryptography Scheme for Halftone Images

S. Meenakumari, S. Nalini
Department of Computer Applications, M.C.A., Anna Universit, Trichy,
Tamilnadu, India

Abstract*— Visual cryptography is a secret sharing scheme which uses images distributed as shares such that, when the shares are superimposed, a hidden secret image is revealed. In extended visual cryptography, the share images are constructed to contain meaningful cover images, thereby providing opportunities for integrating visual cryptography scheme. In this project propose a method for processing halftone images that provides the security while sharing the secret information using extended visual cryptography scheme. The resulting scheme maintains the perfect security of the original extended visual cryptography approach.

Keywords*— visual cryptography, RSA Algorithm, halftone images, Gmail, secure and sharing secret information.

I. INTRODUCTION

With the coming era of electronic commerce applications, there is an urgent need to solve the problem of ensuring information safety in today's increasing open network environment. The encrypting technologies of traditional cryptography are usually used to protect information security. With such technologies, the data become disordered after being encrypted and can then be recovered by a correct key, needing a computational overhead in decryption. Without the correct key, the encrypted source content can hardly be detected even though unauthorized persons steal the data. Visual cryptography, an emerging cryptography technology, uses the characteristics of human vision to decrypt encrypted images. It needs neither cryptography knowledge nor complex computation. For security concerns, it also ensures that hackers cannot perceive any clues about a secret image from individual cover images.

The threshold scheme makes the application of visual cryptography more flexible. With the t out of n threshold scheme (t < n); the manager can first produces n copies of transparency drawn from the secret image, one for each of his members. If any t of them stacks their transparencies together, the content of the secret image will show up. If the number of transparencies is less than t, the content of the secret image will remain hidden. In this approach, a page of cipher text and a printed transparency serves as a secret key. The original text is revealed through placing transparency with key over the ciphered page though they are indistinguishable from random noise. A secret picture must be shared among n participants. The picture is divided into n transparencies so that if m transparencies are placed together the picture is visible. When there are fewer m transparencies it is invisible. This ensures that the secret picture is viewed as a set of black and white pixels with each pixel being handled separately.

Visual cryptography is a unique concept of secret sharing method, in this when the shares are stacked, a hidden secret image is revealed. In extended visual cryptography(EVC), the secret share images are transformed into meaningful shares. EVC with halftone image improves the quality of the recovered secret image and size is equal to the original image. The (k, n)-threshold visual cryptography (VC) scheme is to share a secret image with n participants.

II. PROBLEM DEFINITION

Basic 2-out-of-2 or (2; 2) visual cryptography scheme produces 2 share images from an original image and must stack both shares to reproduce the original image. More generally, a (k; n) scheme produces n shares, but only requires combining k shares to recover the secret image. To preserve the aspect ratio for the recovered secret image for a (2; 2) scheme each pixel in the original image can be replaced in the share images by a 2 X 2 block of subpixels. if the original pixel is white, one of six combinations of share pixels is randomly created. Similarly, the possible share combination for black pixels is also shown. After stacking the shares with white transparent and black opaque, the original secret image will be revealed. Stacking can be viewed as mathematically ORing, where white is equivalent to "0" and black is equivalent to "1". Note that the resulting share images and the recovered secret image contain 4 times more pixels than the original image (since each pixel of the original image was mapped to four subpixels). It may also be noted that the recovered image has degradation in visual since a recovered white pixel is actually comprised of 2 white and 2 black subpixels, while a black pixel is represented by 4 black subpixels in the recovered image.

III. PROPOSED SYSTEM

To propose a method for processing halftone images that improves the quality of the share images and the recovered secret image in an extended visual cryptography scheme for which the size of the share images and the recovered image is the same as for the original halftone secret image. The resulting scheme maintains the perfect security of the original extended visual cryptography approach.

IV. ALGORITHM AND TECHNIQUES

RSA Algorithm:

RSA is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1977. Clifford Cocks, an English mathematician working for the UK intelligence agency GCHQ, had developed an equivalent system in 1973, but it was not declassified until 1997.

A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message.[2] Breaking RSA encryption is known as the RSA problem; whether it is as hard as the factoring problem remains an open question.

RSA is a relatively slow algorithm, and because of this it is less commonly used to directly encrypt user data. More often, RSA passes encrypted shared keys for symmetric key cryptography which in turn can perform bulk encryption-decryption operations at much higher speed.

Operation

a. The RSA algorithm involves four steps: key generation, key distribution, encryption and decryption.
b. RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. The intention is that messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.
c. The basic principle behind RSA is the observation that it is practical to find three very large positive integers e,d and n such that with modular exponentiation for all m:
    1. {\displaystyle (m^{e})^{d}\equiv m{\pmod {n}}
    i. And that even knowing e and n or even m it can be extremely difficult to find d.
d. Additionally, for some operations it is convenient that the order of the two exponentiations can be changed and that this relation also implies:
    1. {\displaystyle (m^{d})^{e}\equiv m{\pmod {n}}}

Key distribution

To enable Bob to send his encrypted messages, Alice transmits her public key (n, e) to Bob via a reliable, but not necessarily secret route. The private key is never distributed.

Encryption

a. Suppose that Bob would like to send message M to Alice.
b. He first turns M into an integer m, such that $0 \leq m < n$ and gcd(m, n) = 1 by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext c, using Alice's public key e, corresponding to
    i. {\displaystyle c\equiv m^{e}{\pmod {n}}}
c. This can be done efficiently, even for 500-bit numbers, using modular exponentiation. Bob then transmits c to Alice.

Decryption

a. Alice can recover m from c by using her private key exponent d by computing
    i. {\displaystyle c^{d}\equiv (m^{e})^{d}\equiv m{\pmod {n}}}
b. Given m, she can recover the original message M by reversing the padding scheme.

Key generation

a. The keys for the RSA algorithm are generated the following way:
b. Choose two distinct prime numbers p and q.
c. For security purposes, the integers p and q should be chosen at random, and should be similar in magnitude but 'differ in length by a few digits' to make factoring harder. Prime integers can be efficiently found using a primality test.
    i. Compute n = pq.
b) n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
c) Compute $\varphi(n) = \varphi(p)\varphi(q) = (p - 1)(q - 1) = n - (p + q - 1)$, where φ is Euler's totient function. This value is kept private.
d) Choose an integer e such that $1 < e < \varphi(n)$ and gcd(e, φ(n)) = 1; i.e., e and φ(n) are coprime.
e) Determine d as $d \equiv e{-}1 \pmod{\varphi(n)}$; i.e., d is the modular multiplicative inverse of e (modulo φ(n))
f) This is more clearly stated as: solve for d given $d \cdot e \equiv 1 \pmod{\varphi(n)}$
g) e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly 216 + 1 = 65,537. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.

h) e is released as the public key exponent.
i) d is kept as the private key exponent.
j) The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and φ(n) must also be kept secret because they can be used to calculate d.
k) An alternative, used by PKCS#1, is to choose d matching $de \equiv 1 \pmod{\lambda}$ with $\lambda = \text{lcm}(p-1, q-1)$, where lcm is the least common multiple. Using λ instead of φ(n) allows more choices for d. λ can also be defined using the Carmichael function, λ(n).
l) Since any common factors of (p − 1) and (q − 1) are present in the factorisation of pq − 1,it is recommended that (p − 1) and (q − 1) have only very small common factors, if any besides the necessary 2.

Signing messages

Suppose Alice uses Bob's public key to send him an encrypted message. In the message, she can claim to be Alice but Bob has no way of verifying that the message was actually from Alice since anyone can use Bob's public key to send him encrypted messages. In order to verify the origin of a message, RSA can also be used to sign a message.

Suppose Alice wishes to send a signed message to Bob. She can use her own private key to do so. She produces a hash value of the message, raises it to the power of d (modulo n) (as she does when decrypting a message), and attaches it as a "signature" to the message. When Bob receives the signed message, he uses the same hash algorithm in conjunction with Alice's public key. He raises the signature to the power of e (modulo n) (as he does when encrypting a message), and compares the resulting hash value with the message's actual hash value. If the two agree, he knows that the author of the message was in possession of Alice's private key, and that the message has not been tampered with since.

V. ARCHITECTURE

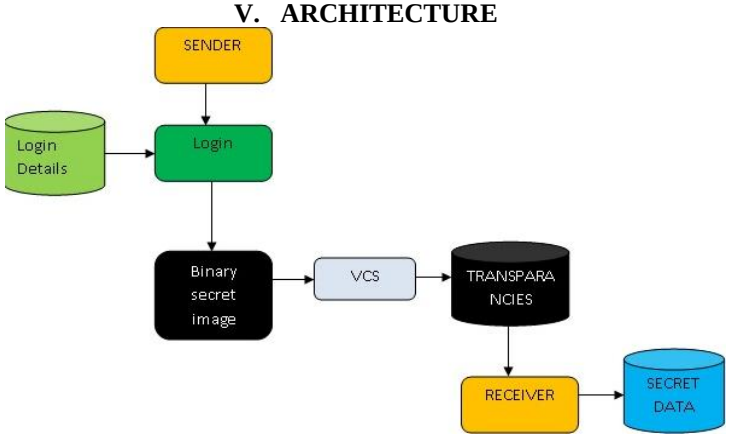

Fig. 1 Overall System Architecture

1. Process of Visual Cryptography Scheme:

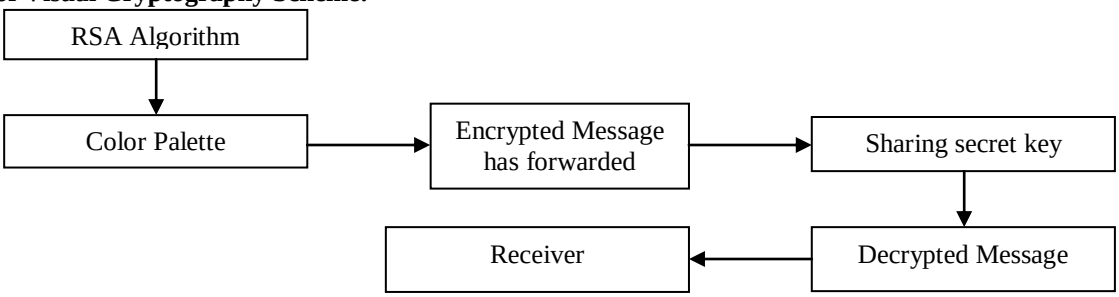

Fig. 2 process of visual cryptography scheme

2. Process of Transparency:

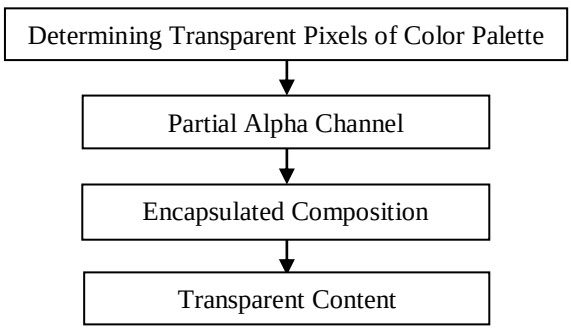

Fig. 3 process of Transparency

VI. MODULE DESCRIPTION

Admin module has a security of visual cryptography and confidentiality of user information. Admin provides the security to their users.

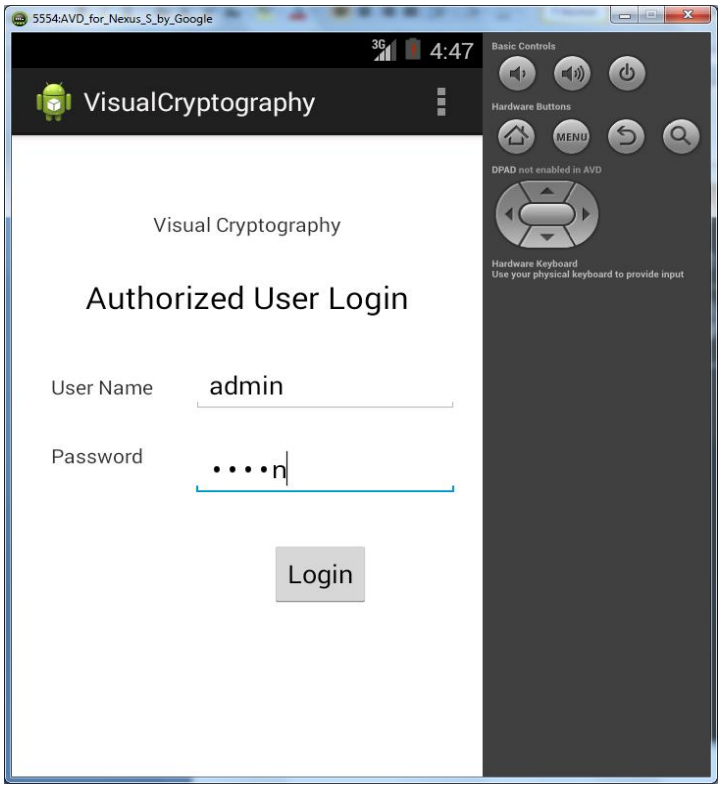

Fig. 4 Admin module of visual cryptography

Admin home page contains the information about the system and its purpose. Admin can view the employee details of the login User. Admin monitoring the user activities through admin view module.

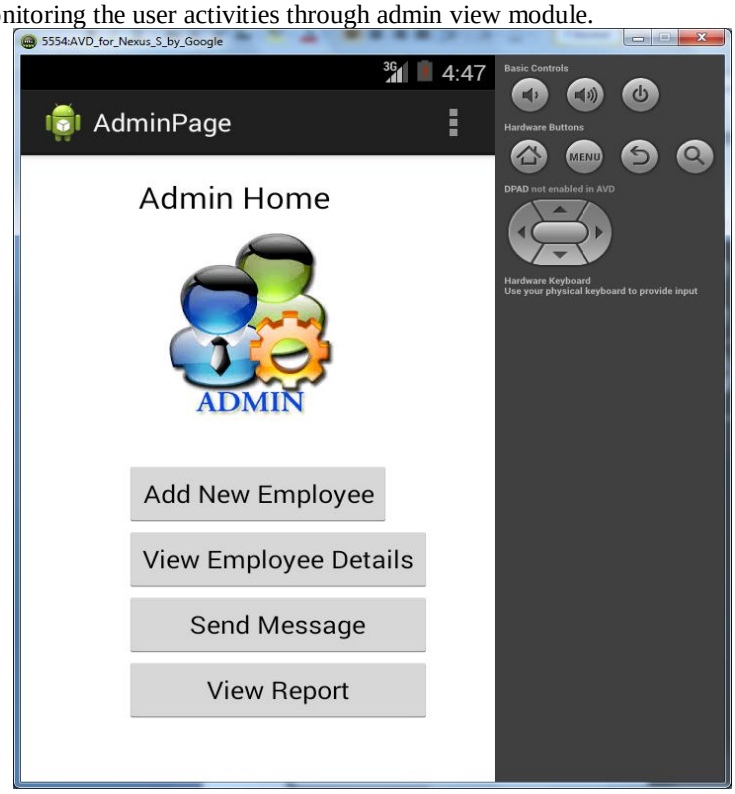

Fig. 5 Admin home page module

Add Employee Details module is taking very important role in registering into their database. Employee Details module can maintain user information in confidential way. This module contains their Registration details like, employee name, mobile no, mail ID, occupation . while registering user details into database automatically it will generate unique id and password to the specific person.

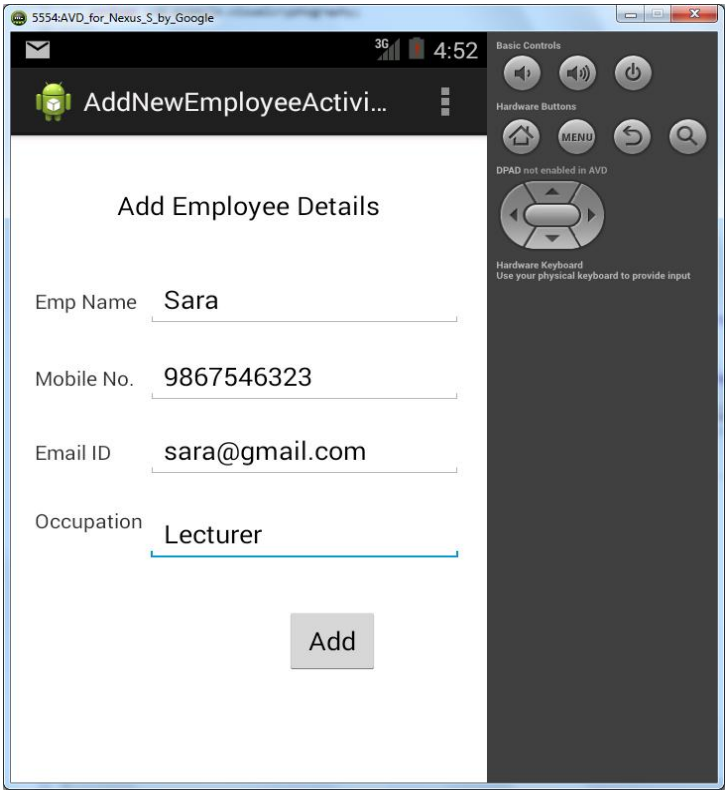

Fig. 6 PG Add Employee Details Module

EMAIL Activity module helps the administrator to send prior notification about unique id and password to the specific person via EMAIL rapidly and an instant communication between user and administrator is possible here to avoid the hacking and falsification.

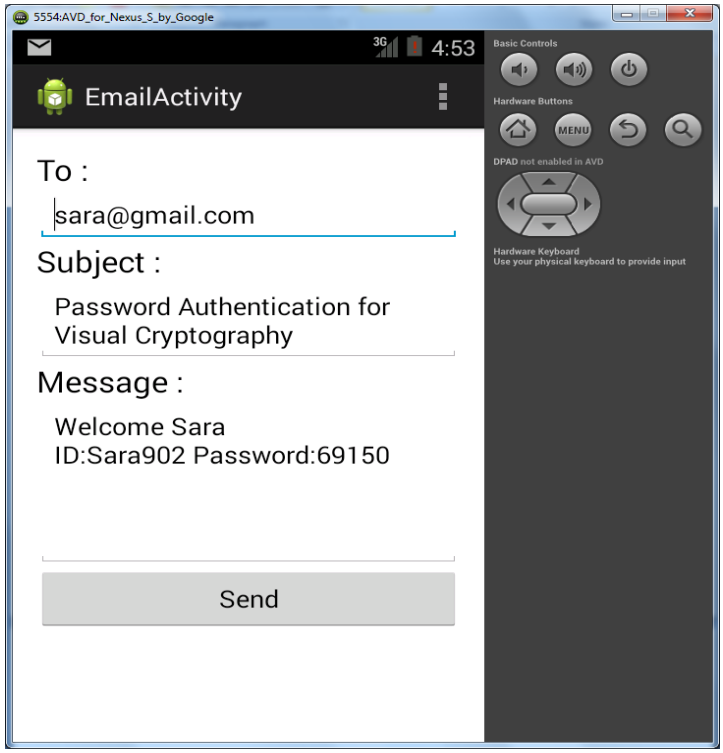

Fig. 7 Email Activity module

Send Message Module helps the administrator to send the secret information to the specific person with the help of visual cryptography. VC is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. RSA is an algorithm used by modern computers to encrypt and decrypt messages. It contains the fields like date, staff id, staff name, message. This module helps the administrator to encrypt the messages while sending and also generate the message id and secret key using an RSA algorithm in a efficient manner which provides the security for sharing secret information.

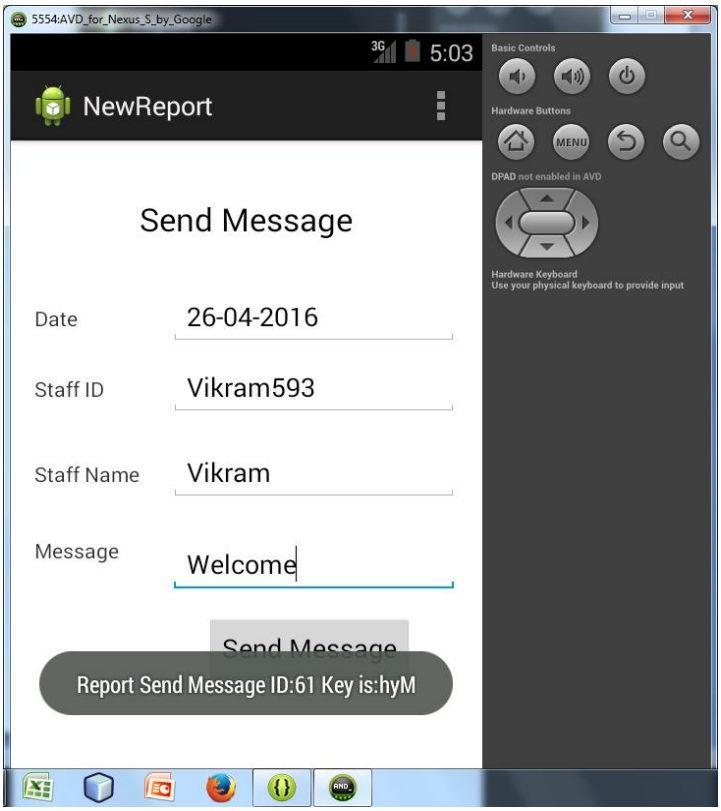

Fig. 8 Send Message Module

Here, user can login with their unique id and password.

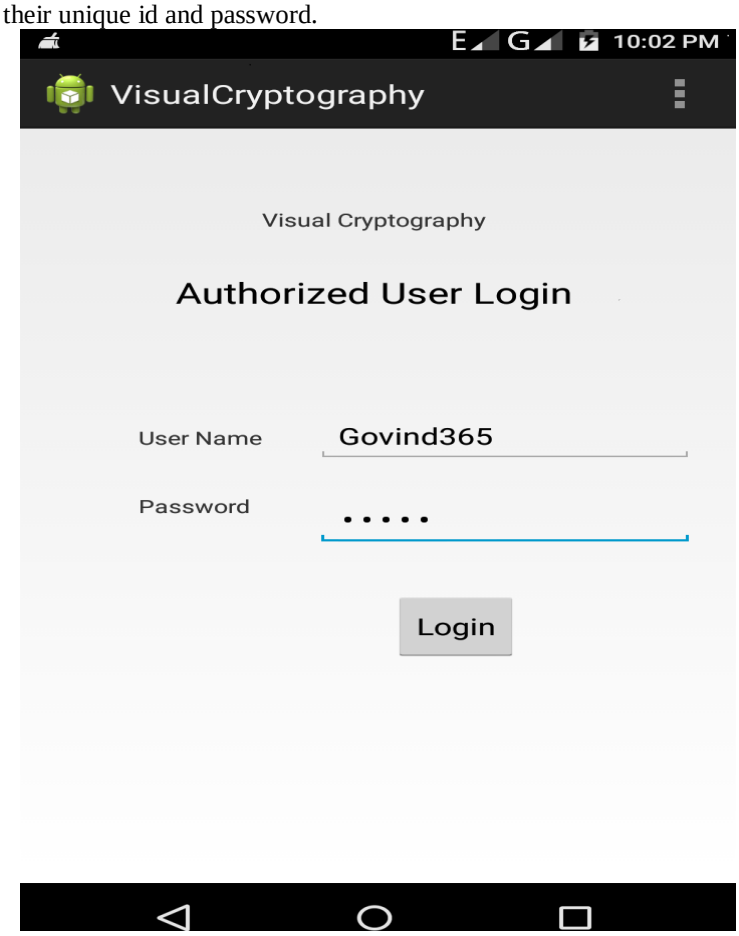

Fig. 9 user Login

VIEW REPORT MODULE Here, the user can receives the meaningful cover images which are meant to be halftone images. In this module user can receives the messages by which is based on RSA algorithmic procedure. The registered user can receive the messages through the cryptographic methodology.

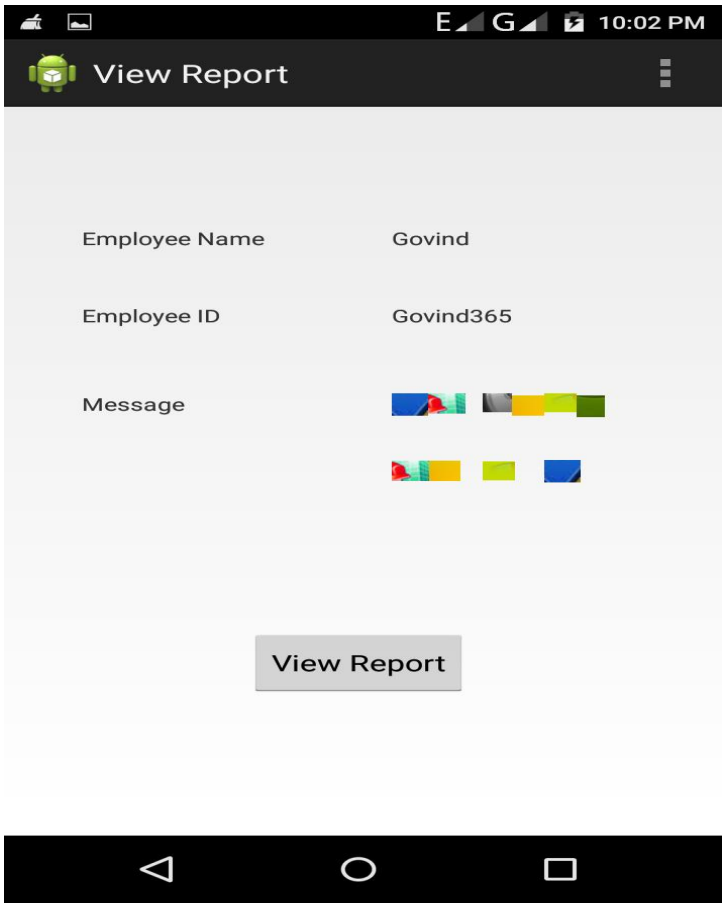

Fig. 10 View Report module

Message authentication module here, the user can decrypt the messages using message id and secret key. The visual secret sharing (VSS),which attempts to reveal the secret image via the human perception of visual system by stacking two or more share. Visual cryptography is a unique concept of secret sharing method, in this when the shares are stacked, a hidden secret image is revealed.

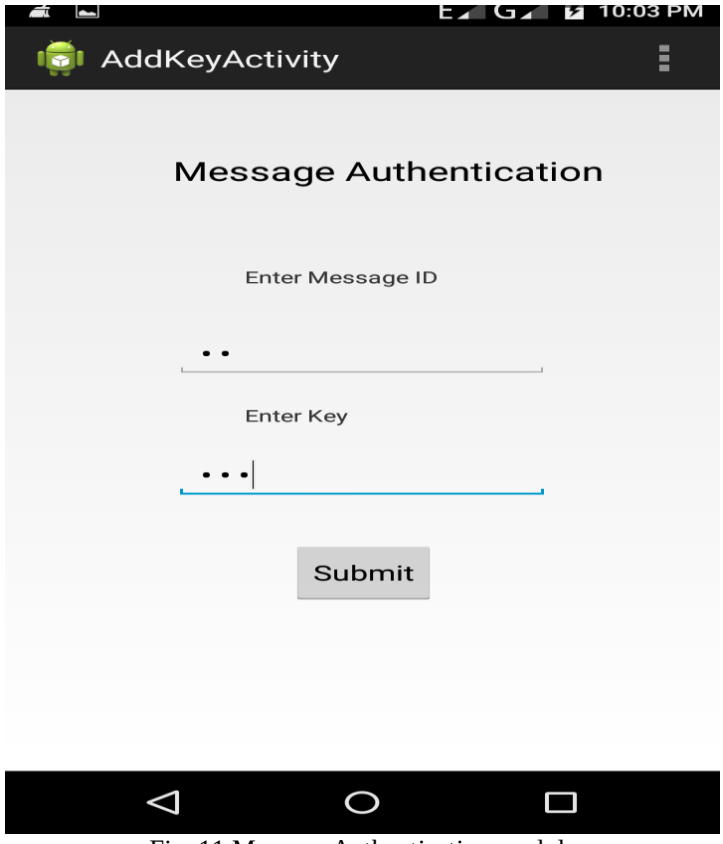

Fig. 11 Message Authentication module

Finally, after all the process of decryption the halftone images are revealed. Now, user can view the secret information.

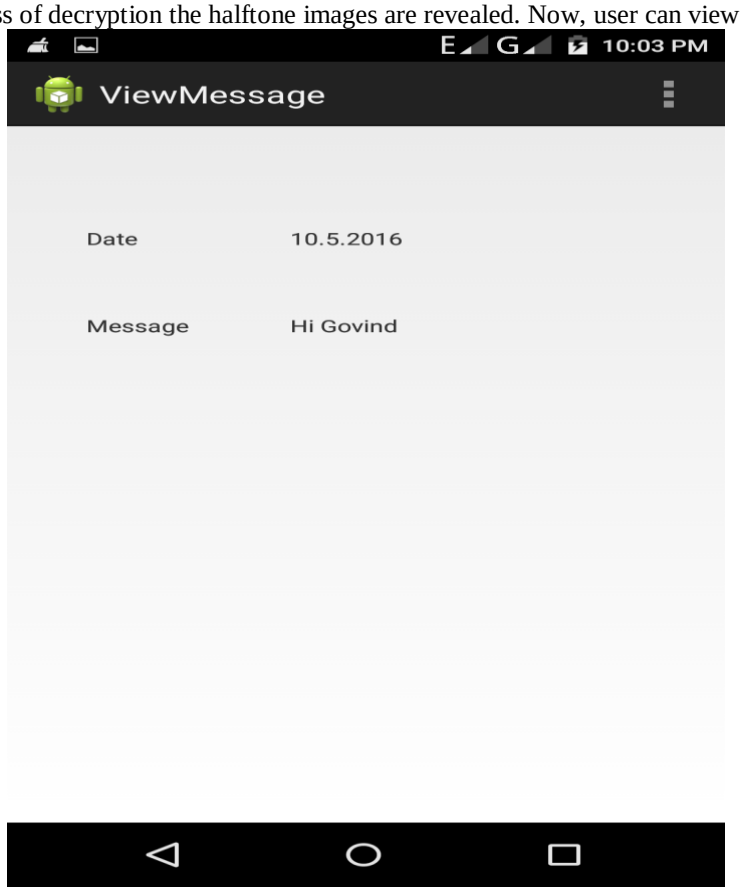

Fig. 12 View Message

VII. CONCLUSION

This work has implemented for secret information sharing to overcome the issues like hacking and falsification. This implementation has resulted in reduction of the computational complexity of a system. Also the security and privacy is enhanced by sharing halftone images with secret keys. So, this paper concludes that applying Extended Visual Cryptography Scheme has not only reduced the falsification but also enhanced the security and privacy of a system by preserving the meaningful cover images in the form of shares.

VIII. FURTHER WORK

This project proposed the extended visual cryptography scheme for natural images. Next it showed a method to improve the image quality of the output by enhancing the image contrast beyond the constraints given by the previous studies. The method enables the contrast enhancement by extending the concept of error and by performing halftoning and encryption simultaneously. The trade-off between the image quality and the security are assessed by observing the actual results of this method. Furthermore, the optimization of the image quality at a given contrast is discussed. Under an assumption that the occurance of the violations is stochastically even in the images, a CFR function is introduced for the image quality optimization. The validity of the assumption and the effect of image quality improvement are also verified with the experiments.

REFERENCE

[1] [E.R.V97] E.R.Verheul and H.C.A.van Tilborg. Constructions and properties of k out of n visual secret sharing schemes. Design Codes and Cryptography, 11(2):179–196, 1997.

[2] [Floyd75] R.W. Floyd and L. Steinberg. An adaptive algorithm for spatial greyscale. Proc.SID, 17/2:75–77, 1975.

[3] [Gomes97] Jonas Gomes and Luiz Velho. Image Processing for Computer Graphics. Springer, 1997.

[4] [Hofme97] T. Hofmeister, M. Krause, and H.U.Simon. Contrast-optimal k out of n secret sharing schemes in visual cryptography. In COCCON ’97, Lecture Notes in Computer Science, volume 1276, pages 176–185, Berlin, 1997. Springer.

[5] [Koga98] Hiroki Koga and Hirosuke Yamamoto. Proposal of a lattice-based visual secret sharing scheme for color and gray-scale images. IEICE Transaction on Fundamentals, E81-A(6):1262–1269, June 1998.

[6] [Naor95] M. Naor and A. Shamir. Visual cryptography, advances in cryptology. Eurocrypt ’94 Proceeding LNCS, 950:1–12, 1995.

[7] [Naor96] M. Naor and A. Shamir. Visual cryptography ii: Improving the contrast via the cover base. Theory of Cryptography Library, (96-07), 1996.

