International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 03, March-2015

Visual Cryptography Schemes for Secret Color Image Sharing using General Access Structure and Stamping Algorithm

Rutuja Kale.[1],
[1]Dept. of Information Technology,
Bhivrabai Sawant Institute of Technology & Reseach,
Pune, India

Nikita Dumbhare[2]
[2] Dept. of Information Technology,
Bhivrabai Sawant Institute of Technology & Reseach,
Pune, India

Prof. Nilesh Thorat[3]
[3] Dept. of Information Technology,
Bhivrabai Sawant Institute of Technology & Reseach,
Pune, India

***Abstract* - Visual Cryptography Schemes (VCS) is a technique of image encryption novel to hide the secret information in images. In the established VCS, the secret image is encrypted into n number of shares arbitrarily and extend to the n number of participates. The secret image can be recovered basically by stacking the shares lacking any complex calculation concerned. However previous approach suffers a safety, pixel extension and noise trouble. The projected scheme consists of two phases. The input secret image generates the n meaningless shares based on General access structure algorithm is complete in the primary phase, at the sender side. The envelop images are added in every share honestly by using stamping algorithm and scattered the embedded images to the participants, in the second phase.**

The entrenched images can be processed to haul out the layer images from the generated shares and the secret images can be retrieved by overlapping the shares in the accurate order, at the receiver side. The secret word verification is also provided at both the sender and receiver side. The proposed system provides high security, increase in the number of shares and reduce the pixel expansion problem and high resolution to visualize the secret image

Keywords: Visual cryptography scheme, General Structure algorithm, stamping algorithm, Shares, transparencies.

1. INTRODUCTION

Visual cryptography, introduced through Naor and Shamir in 1995, is an innovative cryptographic system where the image is decoded by the human illustration system. Thus, there is no need to any complex cryptographic calculation for decryption. The proposal is to hide a secret message (text, handwriting, picture, etc…) in different images called shares or cover images. When the shares (transparencies) are overlap together in order to line up the sub pixels, the secret message can be recovered. The simplest case is the 2 out of 2 scheme where the secret message is hidden in 2 shares, both required for a unbeaten decryption. This can be further extended to the n out n scheme where a secret message is encrypted into n shares. Few years later, Verheul and Tilborg developed a system that can be useful on colored images. The inopportune with these new schemes is that they use meaningless shares to hide the secret and the quality of the recovered plaintext is bad. More advanced schemes based on visual cryptography were introduced in where a colored image is hidden into multiple meaningful cover images. new colored secret sharing and hiding scheme based on Visual Cryptography schemes (VCS) where the conventional overlapping operation of sub pixels and rows interrelations is customized. This novel method does not require transparencies stacking and hence, it is more convenient to use in existent applications. We develop a novel technique that enables visual cryptography of color as well as gray-scale images. With the use a novel encoding scheme, the technique has a unique flexibility that enables a single encryption of a color image but enables three types of decryptions on the same cipher text. The three different types of decryptions enable the recovery of the image of varying qualities. The physical transparency stacking type of decryption enables the recovery of the traditional visual cryptography quality image. An enhanced stacking technique enables the decryption into a halftone quality image. Finally, a computation-based decryption scheme makes the perfect recovery of the original image possible. Based on this basic scheme, we establish a progressive mechanism to share color images at multiple resolutions. We extract shares from each resolution layer to construct a hierarchical structure; the images of different resolutions can then be restored by stacking the different shared images together. Thus, our technique enables flexible

decryption. We implement our technique and present results.

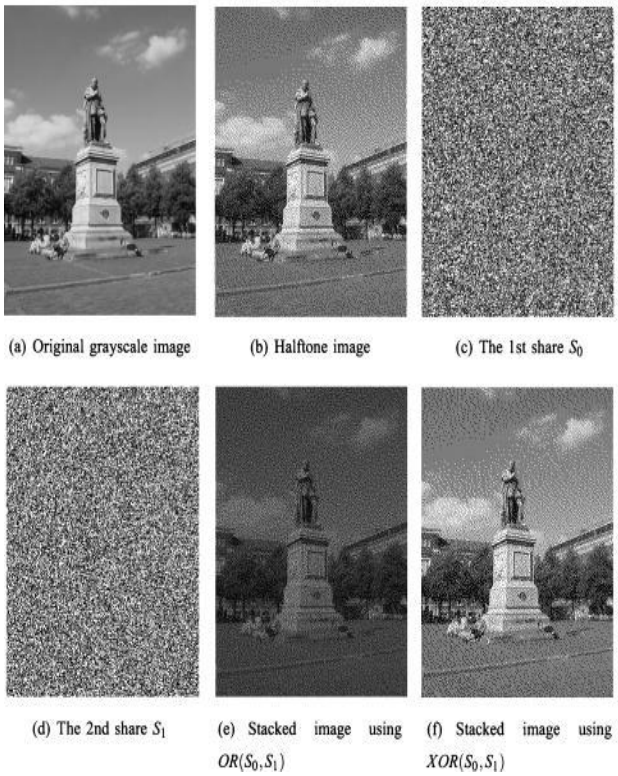


Figure.1. Example of traditional (2, 2)-VCS with image size 128x128.

2. EXISTING SYSTEM

In existing 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. In existing system it take input as black and white image.

2.1 Drawbacks:

The technique which is used to transmit or deliver the secret image over the network is known as visual secret sharing scheme. The major drawback of this scheme is that it suffers from high transmission risk as the shares are like noise which causes the attackers attention and the shares can be intercepted.

3. PROBLEM STATEMENT

The main motto is to provide the high security, increase in the number of shares and reduce the pixel expansion problem and high resolution to visualize the secret color image. Information send through any network have a chance to attack by Intruders. Encryption provides an obvious approach for information security, and encryption programs are readily available. The encryption provides a desirable form to send information without anyone even noticing that information has been sent secret information.

4. PROPOSED SYSTEM

Then data is divided into two or more halves and sent through multiple network channels. Once the data reaches the exact destination all the bits of the actual file which was divided get overlapped on overlap command. When the decode command is used, the original data gets retrieved. It provides a high-level security.

4.1 Our plan and its Advantages:

- Registration for users for security.
- Provides pool details to the user.
- User-Friendly.
- Provide high security for authentication
- Increase in the number of shares
- Reduce the pixel expansion problem and high resolution

5. System Requirement

A) Hardware Components

Monitor: 14” color
Processor: Pentium Celeron
Processor speed: 850 MHz
Memory Size: 1GB MB
Hard Disk Drive: 40 GB
LAN: connect with two system

B) Software Requirements

Operating System: Windows 7
Front End: JAVA
Tools: Eclipse

5.1 JAVA

Java is an object-oriented programming language developed by Sun Microsystems a company best known for its high end UNIX workstations. Java language was designed to be small, simple, and portable across platforms, operating systems, both at the source and at the binary level, which means that Java programs (applet and application) can run on any machine that has the Java virtual machine (JVM) installed.

5.2 J2EE

Java Platform, Enterprise Edition or Java EE is a widely used platform for server programming in the Java programming language. The Java platform (Enterprise Edition) differs from the Java Standard Edition Platform (Java SE) in that it adds libraries which provide functionality to deploy fault-tolerant, distributed, multi-tier Java software, based largely on modular components running on an application server.

5.3 Tomcat Sever 5.5

A Number of servlet containers are available today. The most popular one & the one recognized as the official servlet/JSP container is Tomcat originally designed by Sun Micro Systems Tomcat by itself is a web server this means that you can use Tomcat to service HTTP request for servlets as well as static files(HTML, image files & so on). Tomcat 5.5 uses the Jasper 2 JSP Engine to implement the Java Server Pages 2.0 specification.

- *JSP Custom Tag Pooling* - The java objects instantiated for JSP Custom Tags can now be pooled and reused. This significantly boosts the performance of JSP pages which use custom tags.
- *Background JSP compilation* - If you make a change to a JSP page which had already been compiled Jasper 2 can recompile that page in the background. The previously compiled JSP page will still be available to serve requests. Once the new page has been compiled successfully it will replace the old page. This helps improve availability of your JSP pages on a production server.

5.4 Development Tools

Eclipse & Android SDK Tools are an integrated development environment (IDE) for visually designing, constructing, testing, and deploying Web services, portals, and Java (J2EE) applications.

5.4.1 Eclipse

In computer programming Eclipse does a multi-language I integrated development environment (IDE) comprise a base workspace and an extensible plug-in system for customizing the environment. It is written mostly in Java. It can be used to develop applications in Java and, by means of various plug-INS, other programming language including Ada, C, C++, COBOL, FORTRAN, Haskell, JavaScript, Lasso, Perl, PHP, Python, Ruby, Scala, Clojure, Groovy, Scheme, and Erlang. It can also be used to develop packages for the software Mathematical. Development environments include the Eclipse Java development tools (JDT) for Java and Scala, Eclipse CDT for C/C++ and Eclipse PDT for PHP, among others. The initial codebase originated from IBM Visual Age. The Eclipse software development kit (SDK), which includes the Java development tools, is meant for Java developers. Users can extend its abilities by installing plug-ins written for the Eclipse Platform, such as development toolkits for other programming languages, and can write and contribute their own plug-in modules. Released under the terms of the Eclipse Public License, Eclipse SDK is free and open source software (although it is incompatible with the GNU General Public License). It was one of the first IDEs to run under GNU Class path and it runs without problems under Iced Tea.

5.5 Database platform – My SQL

The world's most widely used open-source relational database management system (RDBMS) that runs as a server providing multi-user access to a number of databases My SQL is a popular choice of database for use in web applications, and is a central component of the widely used. The MY SQL is the open source database.

5.6 Design tool – Star UML Software Modelers

Star UML supports most of the diagram types specified in UML 2.0. It is currently missing object, package, timing and interaction overview diagrams (though the first two can be adequately modeled through the class diagram editor).Star UML supports most of the diagram types specified in UML 2.0. It is currently missing object, package, timing and interaction overview diagrams (though the first two can be adequately modeled through the class diagram editor).

6. NON-FUNCTIONAL REQUIREMENTS

Describe user-visible aspects of the system that are not directly related with the functional behavior of the system. Non Functional requirements include quantitative constraints, such as response time (i.e. how fast the system reacts to user commands.) or accuracy (i.e. how precise are the systems numerical answers.)

6.1. Functional Requirements

Functional requirements specify which output file should be produced from the given File for each functional requirement a detailed description of all data inputs and their source and the range of valid inputs must be specified.

6.2. Security Requirements

The Administrator password must be highly confidential. The users-id must also be confidential. The users should not reveal their id to others as it may lead to wrong usage of account.

7. BASIC CONCEPT

The architecture design describes the overall flow of the system and it is very much important to develop the project by the developers. It explains all the main process such as generate shares, embedding process and extraction process along with its sub process in blocks. The architectural diagram is shown in figure 2.system architecture. In general, three main processes are implemented in this system. At the sender side, the preprocessed secret image can be encrypted by using the GAS solver algorithm. This

image can be protected by using the password authentication. The share synthesizer splits the image into the number of shares as per the number of participants can be done in the generate shares phase. At the embedding phase, the shares can be stamped with the covering images. The embedded images are now ready to send it to the receiver. At the receiver side, the shares can be extracted from the covering images. Thus by overlapping the shares in an order with the correct password verification, the secret image can be retrieved at the extraction phase.

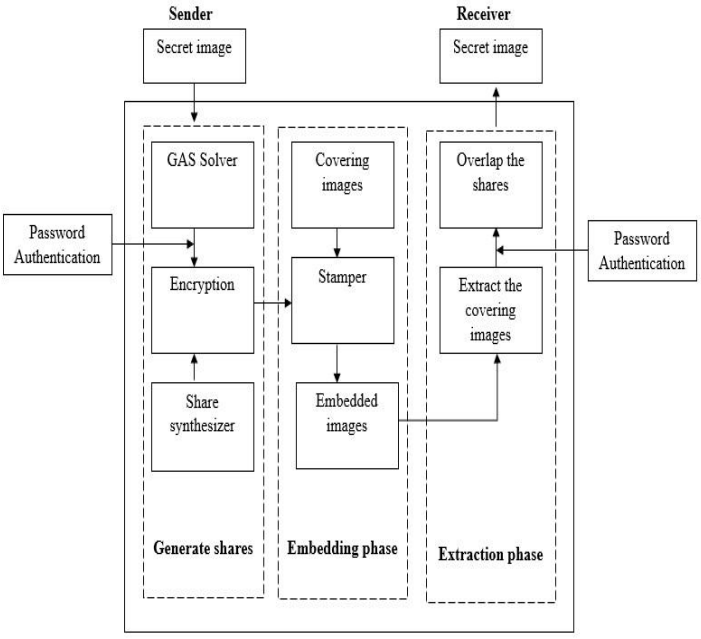


Figure 2.System Architecture

1) Generation of Shares

The algorithm starts to find a solution for the given GAS by the procedure access structure () with an initial set of participants and number of participants in Steps 1 and 2. In each iteration of Steps 3, the algorithm proceeds to find a minimum n‟ by decreasing or increasing the value of n‟ by 1 where n is the number of shares and n' is the number of participants. If a solution is found (i.e., C<=Cbest denotes the best-found energy function in the last iteration), the algorithm stops while n‟ n'-1 or it decreases the value of n‟ by 1 and proceeds to the next iteration with the lower n‟. On the contrary, if a solution is not found, the algorithm stops while n‟< n or it increases the value of n‟ by 1 and proceeds to the next iteration while n‟>n. At the end of the procedure, the algorithm outputs a minimum n‟ and a construction set C as the optimal solution of the problem. If no solution can be found for a given access structure, the solution procedure will be terminated while n=n<=max, where n<=max is a given parameter that prevents Algorithm 2 from falling into an infinite loop. The output of the algorithm produces the qualified shares from where the secret image is hidden in it.

Algorithm 2: SA-based algorithm for GAS solver

INPUT: Set of participants P= {i1, i2… in} and an access structure (TQual, TForb)
OUTPUT: Constructed qualified shares {S1, S2… Sn}
METHOD:
1: Sender set the number of participants P= {i1, i2… in}.
2: The qualified and forbidden set has to be declared.
3: The secret image is splinted into the number of shares as mentioned.
If n<=nmax then Stop and Output “No solution found” Else C <= Cbest
Until n‟= n‟-1
4: Until the number of shares „n‟, the share synthesizer generates the shares
5: The generated share is sent to the embedding process
After getting the secret image, share synthesizer generates the number of shares as per the number of participants and the

2) The Embedding Process

The Embedding process involves embedding the binary image with the covering shares. For that, the covering shares can be divided into the blocks which contain the sub pixels each. Embedding is nothing but the pixels in the embedding positions are replaced by the sub pixels of the share matrix. The input for the embedding process is the covering shares constructed to the corresponding VCS with the covering images required.

Algorithm 3: Stamping Algorithm
INPUT: Shares and covering images
OUTPUT: Embedded image
METHOD: Procedure Stamping (shares, cover images)
1: Calculate the collection of pixel colors for shares, cover images and secret image in coordinate (x, y)
2: Calculate required amount of cover pixels in shares in black and white region of the secret image
3: Calculate the amount of black pixels overlapped at coordinate (x, y)
STEP 4: Set the indicator for coordinate to 0 i.e.., available for stamping cover pixel.
STEP 5: Add cover pixels on selected coordinates (x, y) of shares. The black pixels will be added on candidate coordinate (x, y) of share that has a white pixel on it.
STEP 6: Repeat from step 3 to step 5 until all require cover pixels are stamped on shares

3) Recover Images.

Extract the embedded cover images and secret shares. By stacking the shares in the correct order will get an original secret image is done using the algorithm 4. At the receiver side they stack the shares by using the logical or operation and extract an original secret image. The beauty of such a scheme is that a set of qualified participants is able to recover the secret image

Algorithm 4: Extraction Process
INPUT: Embedded images
OUTPUT: Secret image
METHOD:
STEP 1: Extract the covering images and the shares from the stamped images
STEP 2: Overlap the shares in the appropriate order with authenticated password
STEP 3: The exact secret image can be obtained at the receiver side.
STEP 4: If the order changes or fetching an unauthenticated password leads to retrieve a forbidden image.

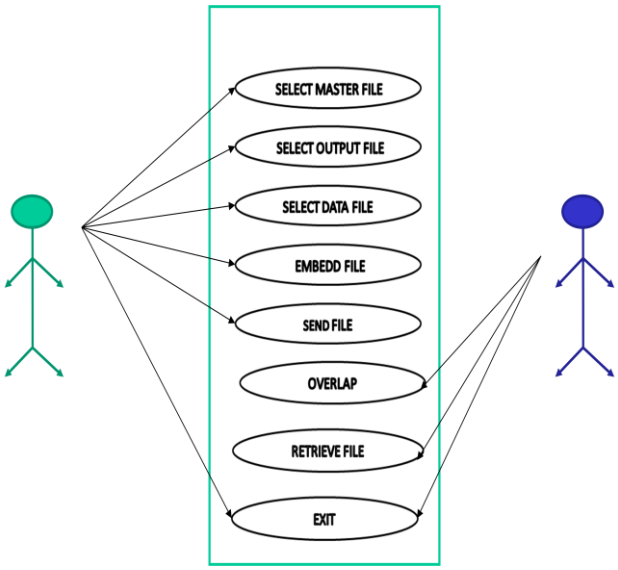
The embedded images are stored in the Embedded Images folder. It is used while the extraction operation is performed. At receiver side, the covering images are extracted from the embedded images after accepting the correct password.

9. LITERATURE SURVEY

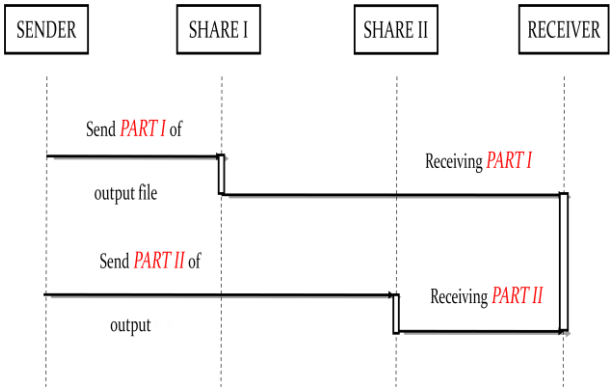
Visual Cryptography Scheme (VCS)
Extended Visual Cryptography Scheme (EVCS). Extended Visual Cryptography Scheme (EEVCS)

10. Design

10.1 Use case Diagram



10.2. Sequence Diagram:



11. EXPERIMENTAL RESULT

Encryption Process:
Source Image: Lena.png
Source image is

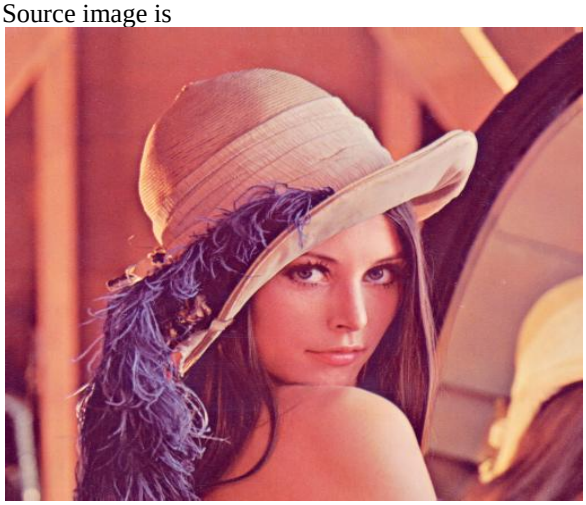


Figure3. Source Image

Number of Shares: 8
Numbers of shares to be taken: 8
The experimental result after encryption by the

Encryption algorithm is given below.

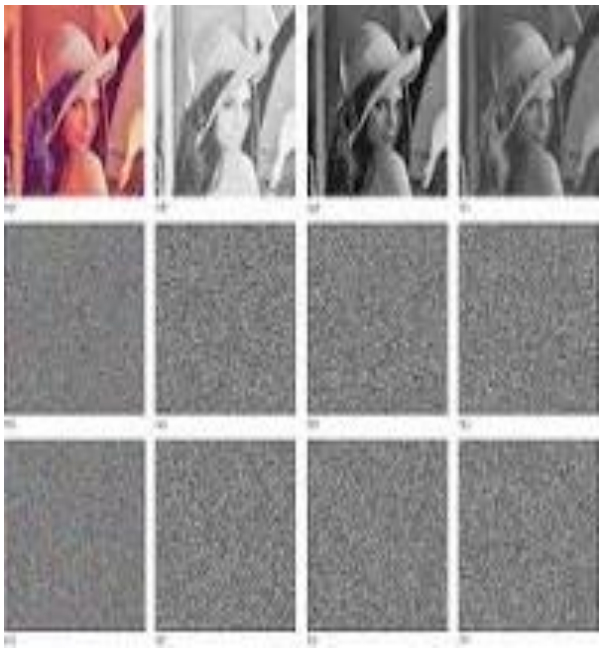


Figure4. Encrypted Share

Decryption Process:
Number of shares: 8
Height and Width of each share: 200, 200
Shares inputted
Final image reconstructed:

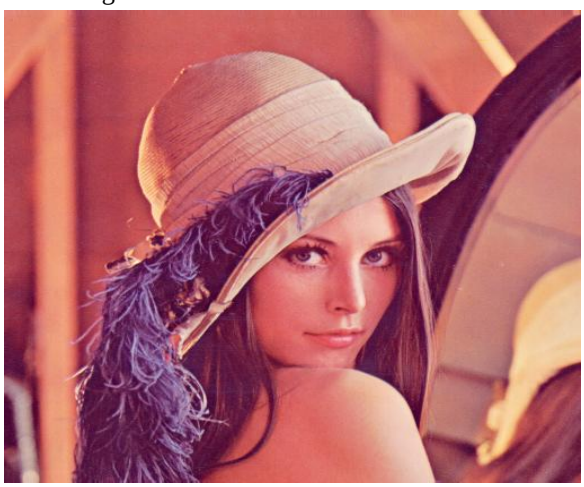


Figure5. Reconstructed Image

16. CONCLUSION

Currently, very few color VC schemes produce meaningful shares, but we consider this a pretty meaningful field of research to explore. In this paper, we offer a new color VC scheme we have developed that generates meaningful shares without increasing the security risks on the secret image. With this proposed scheme, we extend a single pixel into a n block. However, the size of the share remains the same as what happens in the 2×2 pixel expansion case. This way, a considerable part of the storage space can be saved, and more importantly, the shares do not look like random noise. In practical applications, our scheme can be combined with digital watermarking or visual verification systems.

16. FUTURE SCOPE

The future work involves the more number of shares and to implement the secret color Video and share the multiple secret Video by using various methods

17. REFERENCES

1. InKoo Kang, Member, IEEE, Gonzalo R. Arce, Fellow, IEEE, and Heung-Kyu Lee, Member, IEEE, "Color Extended Visual Cryptography Using Error Diffusion", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 20, NO. 1, JANUARY 2011.
2. Shyamalendu Kandar , Arnab Maiti," K-N secret sharing visual cryptography scheme for color image using Random number",vol 3,no.3,Mar 2011.
3. M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1–12.
4. G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Visual cryptography for general access structures," Inf. Comput., vol. 129, no. 2, pp. 86–106, 1996.