IJIIT
International Journal of Infinite Innovations in Technology|ISSN:2278-9057
IJIIT|Volume-IV|Issue-I|2015-2016 July|Paper-01
Reg. No.:20150601|DOI:V4I1P01

IMPLEMENTATION OF IMAGE SLICER WITH STEGANOGRAPHY

Mohan Kumar
Persuing M.E. Dept. of Elect. & Telecom. Engg.
Prof. Ram Meghe Institute Of Tech. and Research
Badnera. Amravati. India
mohankumarji@yahoo.com

Prof. Shrish V. Pattalwar
Associate Professor. Dept. of Elect. & Telecom. Engg
Prof. Ram Meghe Institute Of Tech. and Research
Badnera. Amravati.India
shirishpattalwar@rediffmail.com

Abstract— The Internet serves as an important role for data sharing. However, since it is a worldwide medium, some confidential data might be stolen, copied, modified, or destroyed by an unintended observer. Therefore, security problems become an essential issue. Encryption is a well-known procedure for secured data transmission. Although encryption achieves certain security effects, they make the secret messages unreadable and unnatural or meaningless. These unnatural messages usually attract some unintended observers' attention.

In this paper a new approach has been discussed. This is a combination of Visual Cryptography System (VCS) and Steganography. Visual Cryptography is an encryption technique whereas Steganography is a data hiding technique. Although Visual Cryptography and Steganography techniques have some drawbacks when used independently, our system is able to work very well for short text messages. This has been demonstrated by the various case studies discussed.

Keywords— Visual Cryptography, Steganography, Shares.

I. INTRODUCTION

Visual cryptography is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes, and picture) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers.

Progressive Visual Cryptography (PVC) is a special encryption technique which can be utilized to recover the secret image gradually by superimposing more and more shares. If we only have a few pieces of shares, we could get an outline of the secret image; by increasing the number of the shares being stacked, the details of the hidden information can be revealed progressively. PVC using unexpanded shares regenerates images of high quality.

Steganography is the art and science of communicating in a way which hides the existence of the communication. The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present.

In the proposed method, a new encryption technique is used. This is a combination of Visual Cryptography System (VCS) and Steganography. When these two encryption techniques are used together our system becomes more immune to unauthorized access of secrete text information. Here the secrete text information is encoded in a base image using Steganography. This encoded image is now sliced into multiple shares using Visual Cryptography encryption technique. The encrypted shares are transmitted in an open system enviorement such as the internet. At the receiver end, the received shares are stacked one on top of another to get the encoded image. The secrete text data is decoded from the received image using Steganography technique.

II PROBLEM DEFINITION

In the literature review of a number of papers it has been seen that various authors have encountered numerous problems to transmit information securely over an open ended channel such as the internet.

By using Visual Cryptography, decryption time required by the system can be reduced. Here a less complex system is required ,since in the decryption process the shares have to be stacked one on top of another to generate the secrete image. A system which uses the method of unexpandable shares has been proposed. The contrast of the received image and hence image quality will thus improve. The system will also require less memory.

When shares are transmitted over a channel there is a possibility that hackers may try to decode the image. This is because the shares generate suspicion in the mind of hackers.

To overcome this Steganography technique is used. In Steganography, the text message is hidden in a cover image. By doing so another layer of security has been added in the system. In Steganography secret message is the text data that the sender wishes to remain confidential. This text data is represented by a stream of bits. The cover or host is the medium in which the message is embedded and serves to hide the presence of the message. The cover-image with the secret data embedded is called the "Stego-Image". The Stego-Image resembles the cover image under casual inspection and analysis.

Thus, in the proposed system a number of problems such as only one layer of security, bad image quality, image having low contrast , non graphic user interface, slow systems, capability of handling only monochrome images, static systems, pixel expansion, large memory and a complex systems have been eliminated.

III. IMPLEMENTATION

Our proposed algorithm is implemented in C# .NET framework with Microsoft Visual Studio 2010 (VS).The following steps are followed for secure transmission and reception of text:

Step 1: Encoding of text data- The text data is hidden in a cover image using Steganography

Step 2: Slicing of Image - Get the stego image and divide this image into multiple shares.

Step 3: Stacking the received shares- At the receiver side get all the meaningless shares and stack them together to form original image.

Step 4: Decoding text data-The secrete text data is extracted from the image using Steganography.

IV. APPLICATION WORKFLOW

The following snapshots will guide, how the input text is embedded in a colour image and then the image is sliced into multiple shares.Further we see how the slices are stacked one on top of another to generate the colour image and then the text is extracted from encrypted image.

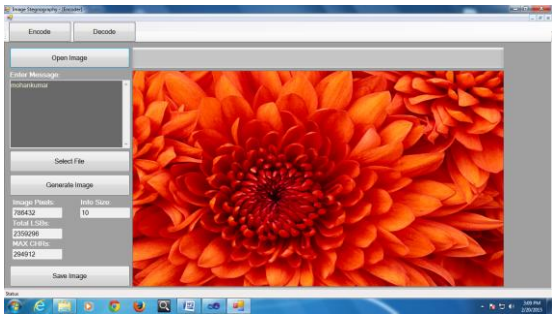

Figure 1 Window after encoding text message.

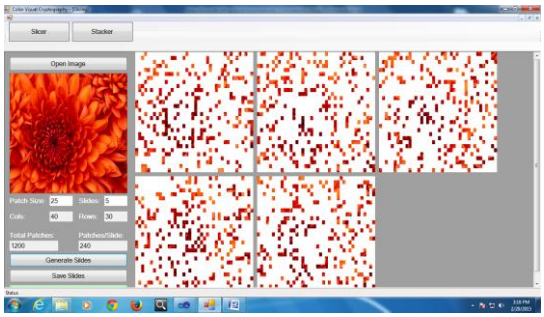

Figure 2 Window after slicing the Image.

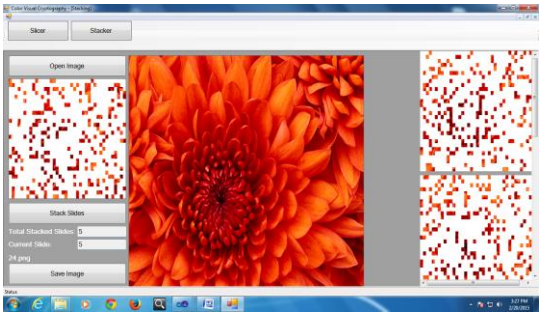

Figure 3 Window after Sacking the slices.

Figure 4 Window after Decoding Text message.

V. Result Analysis

I have applied my proposed framework on a number of different colour images with different text string and have found a set of excellent result set. The images ensure the persistency of their quality. Some of the tested results are as shown.

CASE I

Patch Size 10, Slides 6

Slicer

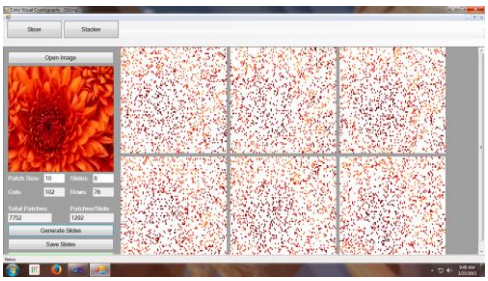

Figure 5 Slicer window for Patch Size 10, Slides 6

Stacker

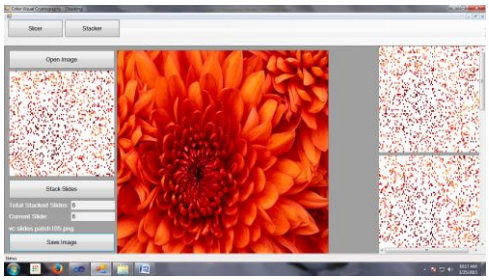

Figure 6 Stacker window for Patch Size 10, Slides 6

CASE II

Patch Size 25, Slides 6

Slicer

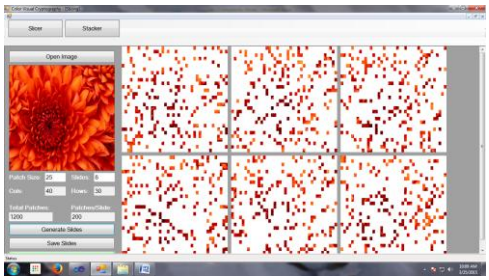

Figure 7 Slicer window for Patch Size 25, Slides 6

Stacker

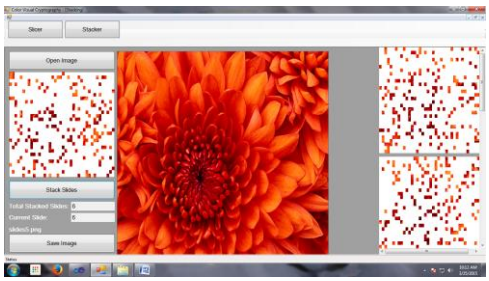

Figure 8 Stacker window for Patch Size 25, Slides 6

CASE III

Patch Size 50, Slides 6

Slicer

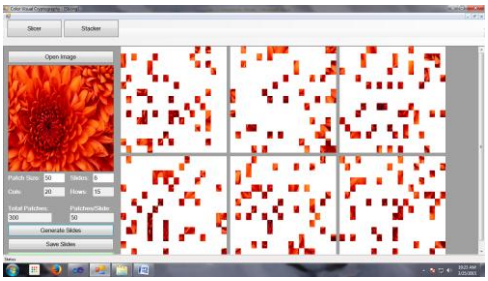

Figure 9 Slicer window for Patch Size 50, Slides 6

Stacker

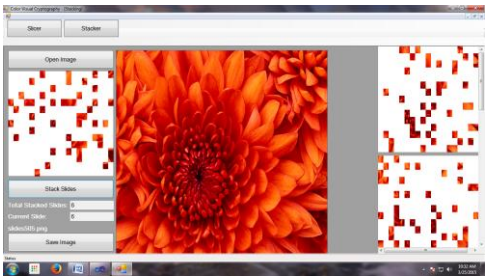

Figure 10 Stacker window for Patch Size 50, Slides 6

CASE IV

Patch Size 100, Slides 6

Slicer

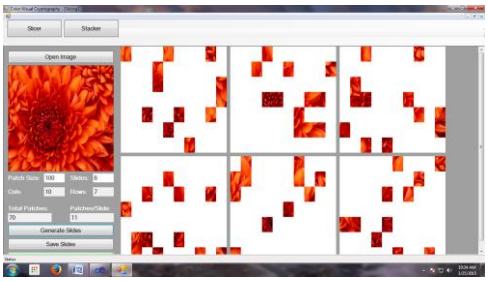

Figure 11 Slicer window for Patch Size 100, Slides 6

Stacker

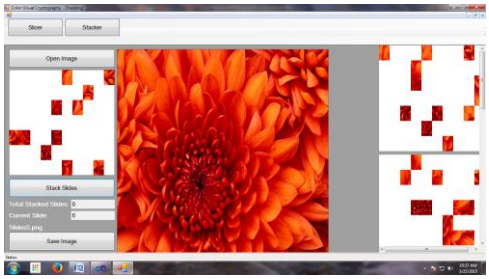

Figure 12 Stacker window for Patch Size 100, Slides 6

CASE V

Patch Size 25 Slides 2 -Slicer

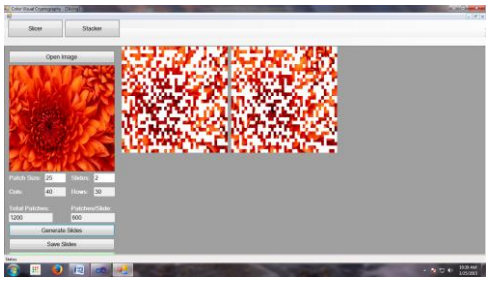

Figure 13 Slicer window for Patch Size 25, Slides 2

CASE VI

Patch Size 25 Slides 4 - Slicer

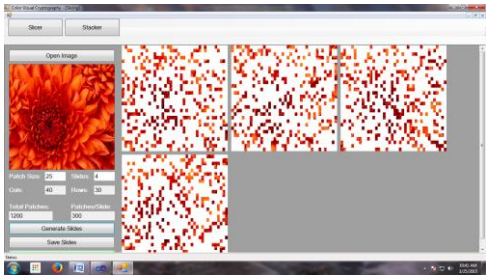

Figure 14 Slicer window for Patch Size 25, Slides 4

CASE VII

Patch Size 25 Slides 6 -Slicer

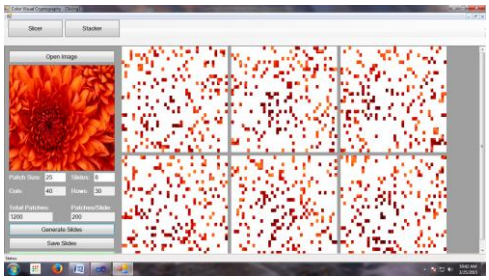

Figure 15 Slicer window for Patch Size 25, Slides 6

CASE VIII

Information Size - 11

Encoder

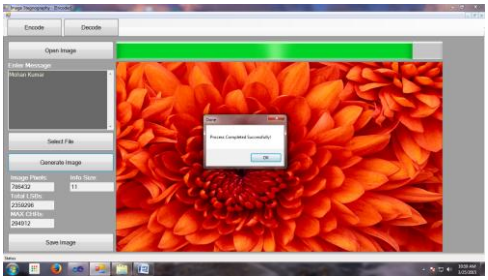

Figure 16 Encoder window for information Size of 11characters

Decoder

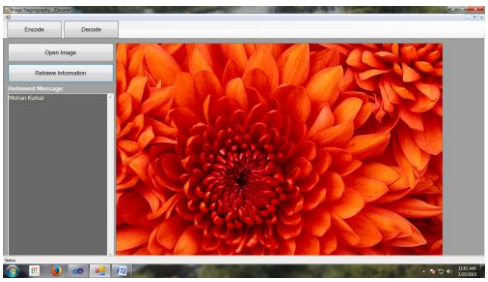

Figure 17 Decoder window for information Size of 11 characters

CASE IX

Information Size – 415

Encoder

Figure 18 Encoder window for information Size of 415 characters

Decoder

Figure 19 Decoder window for information Size of 415 characters

Now we analyze and compare the various parameters obtained from the results.

Table 1 Different parameters obtained when the Patch size is varied but the number of slides are kept constant in the Slicing process.

Serial Number	Patch Size	Number of Slides	Number of Columns	Number of Rows	Total number of Patches	Patches/s
1	10	6	102	76	7752	1292
2	25	6	40	30	1200	200
3	50	6	20	15	300	50
4	100	6	10	7	70	11

We can see in table 1 that when we keep the number of slides constant but vary the patch size, the value of the other parameters change.

Table 2 Different parameters obtained when the patch size is kept constant but the number of slides are changed in the Slicing process.

Serial Number	Patch Size	Number of Slides	Number of Columns	Number of Rows	Total number of Patches	Patches Per slide
1	25	2	40	30	1200	600
2	25	4	40	30	1200	300
3	25	5	40	30	1200	240
4	25	6	40	30	1200	200

We can see in table 2 that when we keep the patch size constant, the number of columns, number of rows and the total number of patches does not change even if we change the number of slides.

Table 3 Different parameters obtained when the Information Size is changed in the Encoding process.

Serial Number	Information Size	Number of Image Pixels	Total LSB	Maximum Characters
1	10	786432	2359296	294912
2	11	786432	2359296	294912
3	4159	786432	2359296	294912

We can see in table 3 that when the size of the text information is increased, the other parameters namely, number of image pixels, total LSB and maximum characters does not change.

The proposed system uses Visual Cryptography and Steganography. I have taken eleven case studies. In these case studies I have changed the size of the patches, number of slides and the size of the text message. In all these cases I was able to receive the text message faithfully. Thus we can say that although Visual Cryptography and Steganography processes may generate some noise, our system is able to circumvent this drawback. This system works very well for short text messages.

VI. CONCLUSION

The proposed system is designed after reviewing the work carried out by various authors on Visual Cryptography and Steganography. Here an enhanced encryption and decryption method has been introduced. This is a combination of Visual Cryptography System (VCS) and Steganography. Both these systems have their own drawbacks but when used together our system becomes more immune to unauthorized access of secrete text information.

REFERENCES

[1] Jthi P.V. and Anitha T Nair. **"Progresive Visual Cryptography with Watermarking for meaningful shares"** ,IEEE,2013.

[2] Young-Chang Hou and Zen-Yu Quan . **"Progressive Visual Cryptography with Unexpanded Shares"** IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 21, NO. 11, NOVEMBER 2011

[3] Soumik Das, Pradosh Bandyopadhyay, Proj Alai Chaudhari and Dr.Monalisha Banerjee, **" A secure key based Digital Text Passing System through Colour Image Pixels"** IEEE International Conference On Advances In Engineering, Science And Management(ICAESM-2012) March 30,31,2012

[4] Joyshree Nath and Asoke Nath "**Advanced Steganography Algorithm using encrypted secret message"** *(IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 2, No.3, March 2011*

[5] Yu-Chi Chen Gwoboa Horng, andDu-Shiau Tsai**" Comment on Cheating Prevention in Visual Cryptography"** IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 21, NO. 7, JULY 2012

[6] Zhi Zhou, R. Arce, and Giovanni Di Crescenzo. **"Halftone Visual Cryptography"** IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 15, NO. 8, AUGUST 2006

[7] Ch.Ratna Babu, M.Sridhar and Dr. B.Raveendra Babu .**"Information Hiding in Gray Scale Images using Pseudo - Randomized Visual Cryptography Algorithm for Visual Information Security",**IEEE. 2013

[8] Silvana and Edlira Martiri.**"Wu-Lee Steganographic Algorithm on Binary Images Processed in Parallel"** International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol: 12 No: 03, June 2013

[9] Shyong Jian Shyu and Hung-Wei Jiang ,**"Efficient Construction for Region Incrementing Visual Cryptography"** ,IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 22, NO. 5, MAY 2012

[10] Xiang Wang, Qingqi Pei, and Hui Li . **"A Lossless Tagged Visual Cryptography Scheme"**
IEEE SIGNAL PROCESSING LETTERS, VOL. 21, NO. 7, JULY 2014

[11] Mamta Juneja and Parvinder Singh Sandhu, (2013) **"A New Approach for Information security using an Improved Steganography Technique",** Journal of Info.Pro.Systems, Vol 9, No:3, pp.405-424.

[12] P.Thiyagarajan, V.Natarajan, G.Aghila, V.Pranna Venkatesan, R.Anitha, (2013) **"Pattern Based 3D Image Steganography",** 3D Research center, Kwangwoon University and Springer 2013, 3DR Express., pp.1-8.

[13] Shamim Ahmed Laskar and Kattamanchi Hamachandran (2013) **"Steganography Based On Random Pixel Selection For Efficient Data Hiding"** ,International Journal of Computer Engineering and Technology, Vol.4,Issue 2.pp 31-44.

[14] S.Shanmuga Priya,K.Mahesh and Dr.K.Kuppusamy,(2012) **"Efficient Steganography Method To Implement Selected Least Significant Bits In Spatial Domain",** International Journal Of Engineering Research And Applications. Vol2 Issue 3.pp 2632-2637