IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Issue-11 E-ISSN: 2347-2693

Design of Arbitrary Image Slicer in Execution of Steganography

A. Balasubramani[1*], Chdv. Subba Rao[2]

[1*]Faculty of Computer Science and Engineering, SIETK, Puttur, India
[2]S.V.U College of Engineering, S.V.University, Tirupati, India

**Corresponding Author: balunbkr@yahoo.co.in*

Available online at: www.ijcseonline.org

Received: 13/Oct/2017, Revised: 25/Oct/2017, Accepted: 14/Nov/2017, Published: 30/Nov/2017

***Abstract*—A** new coding technique is projected in this paper. Steganography and visual Cryptography is employed to achieve the security. The secret colour image is hidden behind a canopy image. The steganographic image is currently sliced into multiple slices and transmitted in an open system setting. At the receiver side, the received slices are organised in such a way that to come up with the original image, that has the secret colour image hidden in it. This can be done by Visual Cryptography. Currently Steganography is employed on this image to get the secret image.

Keywords-Cryptography, Steganography, secret image

I. INTRODUCTION

Cryptography is an encryption technique to shield against unauthorized information access. It is used once human action over associate open complete channel like web, wherever info has to be shielded from third parties. The various aspects of data security like integrity, confidentiality, and non-repudiation and authentication area unit associated with cryptography.

Encryption technique can jointly called secret writing, converts information into associate indecipherable format therefore to shield the knowledge from unauthorized parties. It is helpful in making certain privacy and security of the knowledge transmitted or shared between the systems.

Visual cryptography (VC), planned by Naor and Shamir [1], it's a paradigm for cryptanalytic schemes that permits the secret writing of secret pictures with none advanced cryptanalytic calculation. Significantly in a very k-out-of-n visual secret sharing theme (VSS), a hidden image is encrypted into 'n' no of shares, it then photocopied onto transparencies severally and shared among n participants. Hidden pictures are visually discovered on paper by stacking along any k or a lot of transparencies of the shares.

However, by examining k shares, nobody gets any info concerning the key image, although infinite resources area unit used [17]. At this time we'd like to explain the term 'Steganography'. Steganography merely suggests that, "Covered Writing". Steganography is that the art and science of secret communication that hides the presence of the information [16]. In distinction to cryptography, wherever the unauthorized parties area unit allowed to trace, spoof and alter the message while not being to breach the sure security premise policies arranged by cryptosystem, The aim of Steganography is to cover message or info within any common object in specified it forbid any unauthorized parties or users to acknowledge that there's any sort of secrete message or information gift.

Cryptography and Steganography each area unit supposed to guard the confidential or any sort of data from unauthorized users. Each technique area unit wonderful thanks to accomplish the target of protective hint from anybody.

But no technique of technology is ideal once it's used alone and there could be potentialities of obtaining broken. Owing to this reason, most consultants advocate to use each the technologies to feature extra layers of security to data. Steganography technologies area unit important for the long run of web and Privacy systems on open terminated channel or medium of supply of knowledge viz. web [16]. Steganography analysis is essentially compelled by the lacking strength within the cryptanalytic systems and also that would like possess complete secrecy of knowledge in Associate in Nursing open channel like web.

II. PROBLEM DEFINITION

It has been seen that numerous ways have been encountered to transmit data firmly over in many open terminated channels like the net. By exploitation Visual Cryptography, decoding time needed by the system will be reduced. Here a less complicated system is needed since within the decoding method the slices ought to be organised one on high of another to come up with the secrete image. A system that uses the logic of undependable shares has been projected. The distinction of the received image and thus image quality can therefore improve. The system will need less memory.

When the slice is transmitted over a channel there's a prospect that hackers might attempt to decrypt the image. This can be as a result of the shares generate suspicious within the mind of hackers. To beat this Steganography technique is employed. In Steganography, the secrete image is hidden during a carrier image. By doing this another layer of security has been implemented within the system. In Steganography secret data is totally different colour image that the sender desires it to stay confidential this secrete image is described by a shares. The host or cowl is that the medium during which the secrete image is engulfed and provides the concealment of the existence of the secrete message.

After embedding the key data into carrier image is named the Stegano-Image. The Stegano-Image resembles the duvet image beneath irregular scrutiny and analysis.

Thus, within the projected system variety of issues like just one layer of security, unhealthy image quality, image having low distinction , non-graphic interface, slow systems, capability of handling solely monochrome pictures, static systems, constituent enlargement, massive memory and a fancy systems are eliminated.

The organisation of the paper, in section 2 we discussed problem definition, In section 3 discussed about proposed system, in section 4 discussed about implementation, in section 5 discussed about advantages, in section 6 discussed about applications.

III. PROPOSED SYSTEM

In projected work we have a tendency to style random image slicer for secret colour pictures that uses visual cryptography for secrete image sharing with image Steganography. That divides pictures into n no of shares. By increasing quantity of the shares/slices being stacked, the small print of the hidden info is exposed bit by bit. No one will get any hidden info from one share. This kind of visual cryptography technique is secure because the shares created are senseless pictures and hackers have additional attraction within them as they take into account it as suspicious info in the transmission [8].
In this projected technique, a Steganography technique is employed to get purposeful shares. Thekey colour image shares are hid into some cowl pictures so hackers is pleased from them. Projected technique can offer associate economical thanks to hide the secrete image in purposeful cowl image, that provides high security and recovered image with higher distinction.

In projected technique the initial image is recovered with same size i.e. there's no component enlargement or compression. Briefly there's no modification in image resolution. Therefore, it avoids giant memory needs.

A. cryptography part of random image slicer with steganography (At Sender side):
The secrete colour image is initially divided into n numbers of shares mistreatment Random Image Slicer. Every of those shares are then enclosed into cowl image to supply purposeful shares, that is then on the way through totally different routes [12].

B. secret writing part of random image slicer with steganography (At Receiver side):
In the secret writing method, the initial shares are separated from purposeful shares. This shares are then accumulated along to induce the initial image[12].

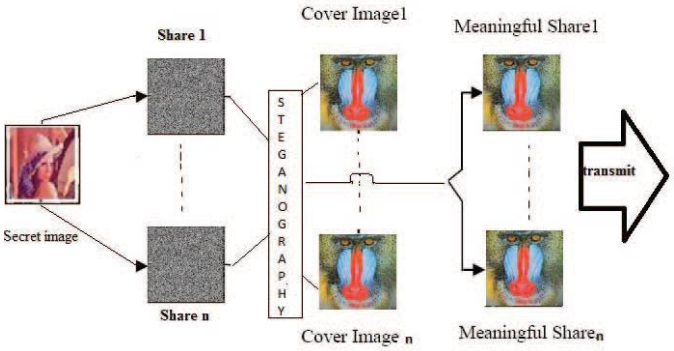


Fig. 1 Encryption segment of random image slicer with Steganography

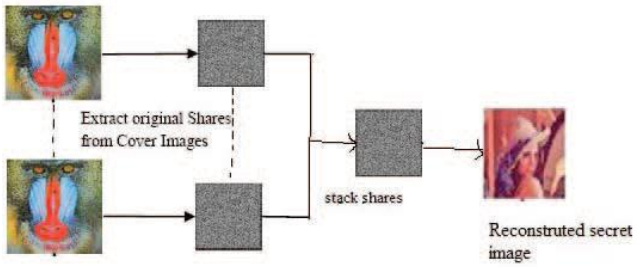


Fig. 2 Decryption segment of random image slicer with Steganography

IV. IMPLEMENTATION

Our projected algorithmic program is enforced in C# .NET framework with Microsoft Visual Studio 2010 (VS).The following algorithmic program steps square measure followed for secure transmission and reception of secrete image:

Proposed algorithmic program for Slicing the first image

Input: Original image, cowl Image patch size, variety of slides
Output: important shares of original pictures.
1. Get original image.
2. Get patch size and obtain total slides.
3. Generate all statistics like,

Cols = breadth / patch size.
Rows = height / patch size.
Total patches = rows * cols.
Patches per slide = total patches / slides.
4. Generate blank slide pictures and store in slide array.
5. Generate XY coordinates of all patches and store inPatch array.
6. Generates patch IDX array for shuffling.
7. Shuffle the array.
8. For (i=0; i<=total patches; i++)
8.1. Fetch the coordinate of x,y of current patch.
8.2. Copy all the pixels of current patch to the Selected slide.
9. Increment slide and attend step eight.
10. Get cowl image.
11. for every constituents of canopy Image XOR each pixel of Slide.
12. Update in new image.
13. Update panel.
14. Save slides

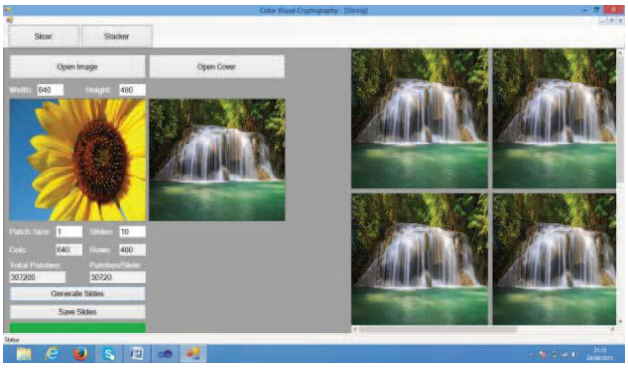


Fig. 3 Slicing Slides Screen.

Input: All purposeful shares of original pictures.
Output: final pictures same as original image.
1. Fetch all the slides from fixed disk.
2. Get cowl image and its size.
3. Get original image size.
4. Fetch the constituent of of canopy image.
5. Fetch the constituent of slide.
6. For (i=o; i<total slides; i++)
6.1. XOR the all the constituent of current slide and canopy image.
6.2. And store in master blank slide.
6.3. OR the all the constituent of current master slide and stacked slide.
7. Increment slide and head to step half-dozen.
8. Update panel.
9. Save image

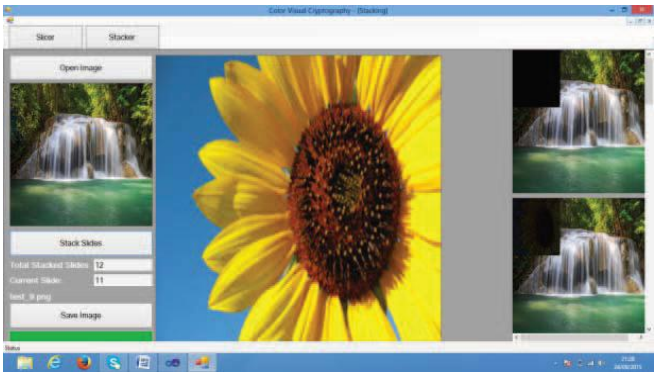


Fig. 4 Stacking Slides Screen.

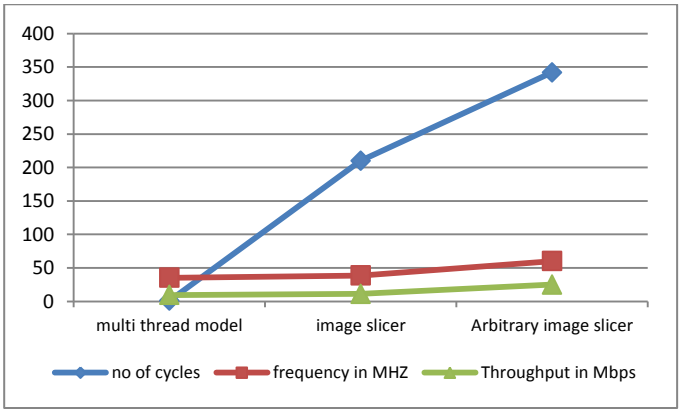
V. ADVANTAGES

1. Capability of handling colour pictures.
2. Extra layer of security accessorial within the system.
3. The secrete image is encrypted into n no of shares in order that cryptography is not possible by human sensory system.
4. Avoid massive memory demand as a result of there's no enlargement.
5. Recover image with high distinction and sensible quality

VI. APPLICATION

This type of visual cryptography methodology square measure to encipher the visual info like written text, written notes, pictures, documents, military maps. This will even be utilized in Biometric system, remote electronic pick, and bank client identification.

	multi thread model	image slicer	Arbitrary image slicer
frequency in MHZ	35.4	38.6	60.2
Throughput in Mbps	9.576	11.174	25.17



VII. CONCLUSION

In this paper, **A** new coding technique is projected Steganography and visual Cryptography is employed to

achieve the security. The secret colour image is hidden behind a canopy image. The steganographic image is currently sliced into multiple slices and transmitted in an open system setting. At the receiver side, the received slices are organised in such a way that to come up with the original image, that has the secret colour image hidden in it. This can be done by Visual Cryptography. Currently Steganography is employed on this image to get the secret image

REFERENCES

[1]. M. Naor and A. Shamir, "*Visual cryptography*," in Proc. Adv. Cryptol.: EUROCRYPT, vol. 950. 1995, pp. 1–12.

[2]. Thomas Monoth and Babu Anto P "*Contrast-Enhanced Visual Cryptography Schemes Based on Additional Pixel Patterns*", 978-0-7695- 4215-7/10 2010 IEEE.

[3].S.Punitha, S. Thompson and N.Siva Rama Ling "*Binary Watermarking Technique based on Visual Cryptography*," 978-1-4244-7770-8/10/ 2010 IEEE.

[4]. E.Sangeetha Devi, "*Enhanced Visual Secret Sharing Scheme via Halftoning Technique",* 978-1-4244-7770-8/10/2010 IEEE.

[5]. Divya.A and K. Ramalakshmi, "*Maintaining the Secrecy in Visual Cryptography Schemes*," 978-1-4244 -8679-3/11/2011 IEEE.

[6]. Ali Makki Sagheer, Salah Sleibi Al-Rawi and Laith hamid Abed, "*Visual Cryptography Technique based on FFT*," 978-0 7695-4593-6/11 2011 IEEE.

[7]. InKoo Kang, Gonzalo R. Arce, "*Color Extended Visual Cryptography Using Error Diffusion",* and Heung-Kyu Lee, 1057 7149/ 2010 IEEE.

[8]. Young-Chang Hou, Zen-Yu Quan, "*Progressive Visual Cryptography with Unexpanded Shares,*" IEEE Transactions on Circuits And Systems For Video Technology, Vol. 21, No. 11, November 2011.

[9]. HAN Yan-yan, Xi'an China, "*A Watermarking-based Visual Cryptography Scheme with Meaningful Shares*," 978-0-7695-4584-4/11 2011 IEEE.

[10].Ch. Ratna babu, M. Sridhar, Dr. B. Raveendra Babu, "*Information Hiding in gray scale Images using Pseudo-Randomized Visual Cryptography Algorithm for visual Information Security*," IEEE International conference on information systems and computer networks, March 2013.

[11].Rajendra Basavegowda and Sheshadri Seenappa, "*Electronic Medical Report Security Using Visual Secret Sharing Scheme*," 978-0-7695-4994- 1/13, 2013 IEEE.

[12].Jithi P V, Anitha T Nair, "*Progressive Visual Cryptography with watermarking for meaningful shares*," by 978-1-4673-5090-7/13/ 2013 IEEE.

[13]. Adi Shamir, "*How to Share a Secret,"* published in ACM, Laboratory for Computer science, Massachusetts Institute of Technology, 1979.

[14]. K. Arora, G. Gandhi, "*A Review of Approaches for Steganography*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.5, pp.118-122, 2014.

[15]. Zhi Zhou, Gonzalo R. Arce and Giovanni Di Crescendo, "*Half tone Visual Cryptography*," IEEE Transaction on image processing, vol.15, no.8, 2006.

