International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 3 Issue: 11
ISSN: 2454-4248
500 – 509

Steganography- A Powerful Web Security Tool for Data Transmission

N.Bhaskar [1]
Research Scholar, Computer Science
Rayalaseema University,
Kurnool, Andhra Pradesh, India
Email: niraghatam@gmail.com

M.V. Ramanamurthy [2]
Professor & Head, Dept. of Mathematics,
MGIT, Gandipet, Hyderabad
Telangana, India
Email: mv.rm50@gmail.com

Rajani Bellamkonda [3]
Asst. Professor, Dept. of Computer Science,
Aurora's Degree and P.G. College
Chikkadapalli, Hyderabad, Telangana, India
Email-id: bkrajani@gmail.com

Ameer Saad Kadhim Al-Mawla [4]
Dept. of Mathematics & Comp. Sci.,
Hyderabad, Telangana, India
Email-id: amsaa834@gmai.com

Abstract : The main objective of this paper titled " **Steganography – A secured tool for web data transmission**" is to provide security for data files during transmission in the network. The main motto of this type of data security is to prevent data access by unauthorized users during data transmission. The steganography is the process to convert the transmitting data in the network in an unreadable format and it is difficult to understand the stolen person.

Keywords : Steganography, ABE-Attribute Based Encryption, AnonyControl-F (a cloud data access control mechanism), Fragile, Robust, LSB-Least Significant Bit, GLS-Generalized Least-Squares Solution, WLS - Weighted Least-Squares.

*****

I. Introduction

In corporate network of clients/server need to interact with each other and parallel maintain the confidentially of data. Before transmission of the encrypts it using the IDEA algorithm and is then sent on the network. The receiver before reading the file needs to decrypt it using the same algorithm to get the actual data. The keys needed to encrypt/decrypt data are pre-known to specific sender and receiver. The information security is not just about the information substance. Steganography is the embedding of messages within an innocuous cover work in a way which can not be detected1 by anyone without access to the appropriate steganographic key. Wikipedia calls steganography, incorrectly, a form of "security through obscurity". This is not true as a correctly designed, key-based system will resist attackers that know the details of the algorithm but not the key. Steganalysis is the study of attacking such systems, analagous to cryptanalysis of cryptographic systems. A threat model consists of a attack scenarios we use to evaluate steganographic techniques. In this paper, the threat model is that of a passive warden — someone who can see and analyze the data but cannot alter it in an attempt to destroy the hidden message. Therefore, the techniques aim to hide the existence of a message, without worrying too much about robustness. Steganography is the embedding of messages within an innocuous cover work in a way which can not be detected1 by anyone without access to the appropriate steganographic key. Wikipedia calls steganography, incorrectly, a form of "security through obscurity". This is not true as a correctly designed, key-based system will resist attackers that know the details of the algorithm but not the key. Steganalysis is the study of attacking such systems, analogous to cryptanalysis of cryptographic systems. A threat model consists of a attack scenarios.

we use to evaluate steganographic techniques. In this paper, the threat model is that of a passive warden — someone who can see and analyze the data but cannot alter it in an attempt to destroy the hidden message. Therefore, the techniques aim to hide the existence of a message, without worrying too much about robustness.

 ISSN: 2454-4248
500 – 509

Subsequent to the most alluring part of the distributed computing is the calculation outsourcing, it is a long ways sufficiently past to simply direct an entrance control. More probable, clients need to control the benefits of information control over different clients or cloud servers. This is on account of when delicate data or calculation is outsourced to the servers may illicitly examine clients' information and access touchy data, or different clients may have the capacity to derive delicate data from the outsourced calculation. Consequently the entrance as well as the operation ought to be controlled. Also, individual data (characterized by every client's properties set) is at danger since one's personality is validated in view of his data with the end goal of access control (or benefit control in this paper).

TYPES OF STEGANOGRAPHY :

Steganography can be split into two types, these are Fragile and Robust. The following section describes the definition of these two different types of steganography. Fragile steganography involves embedding information into a file which is destroyed if the file is modified. This method is unsuitable for recording the copyright holder of the file since it can be so easily removed, but is useful in situations where it is important to prove that the file has not been tampered with, such as using a file as evidence in a court of law, since any tampering would have removed the watermark. Fragile steganography techniques tend to be easier to implement than robust methods.

Robust marking aims to embed information into a file which cannot easily be destroyed. Although no mark is truly indestructible, a system can be considered robust if the amount of changes required to remove the mark would render the file useless. Therefore the mark should be hidden in a part of the file where its removal would be easily perceived.

There are two main types of robust marking.

a) Fingerprinting involves hiding a unique identifier for the customer who originally acquired the file and therefore is allowed to use it. Should the file be found in the possession of somebody else, the copyright owner can use the fingerprint to identify which customer violated the license agreement by distributing a copy of the file.

b) watermarks identify the copyright owner of the file, not the customer. Whereas fingerprints are used to identify people who violate the license agreement watermarks help with prosecuting those who have an illegal copy. Ideally fingerprinting should be used but for mass production of CDs, DVDs, etc it is not feasible to give each disk a separate fingerprint. Watermarks are typically hidden to prevent their detection and removal, they are said to be imperceptible watermarks.

As per the reference of Houidi, I., Mechtri, M., Louati, W., & Zeghlache, D. (2011, July), research presents work-in-advancement on the cloud administration provisioning crosswise over different cloud suppliers. The work accept the development of Cloud Brokers in the middle of clients and cloud suppliers. The representatives part client demands and guarantee provisioning from different suppliers. A careful part calculation is produced to proficiently part the cloud demands among the numerous cloud stages with the point of diminishing the expense for clients. This part is figured as a Mixed Integer Program and this is consolidated with Open Flow and NOX innovations that attain to stream based between cloud organizing. Another controller module is created and incorporated in NOX to arrange the Open Flow switches for between cloud way foundations.

II. Problem Analysis

The study exhibit a semianonymous benefit control plan AnonyControl to address the information security, as well as the client character protection in existing access control plans [1]. Other than the way that we can express discretionarily broad encryption approach, our framework additionally endures the bargain assault towards Attributes powers, which is not secured in numerous current works. The goal of steganography is to avoid drawing suspicion to the transmission of a hidden message. If suspicion is raised, steganography may fail. The success of

 ISSN: 2454-4248
500 – 509

steganography depends on the secrecy of the action. If steganography is detected, the system will fail but data security depends on the robustness of the applied algorithm. In this paper, we compress the secret message and encrypt it by the receiver's public key along with the stego key and embed both messages in a carrier using an embedding algorithm[2]. The stegno - image is the result we get by running the algorithm you select on the message (file to hide) and cover (image). It can be saved into BMP or PNG format. The reason that it can only be saved in these formats is because they are lossless - there is no information lost as part of the file formatting. The various applications of steganography include secure military communications, multimedia watermarking and fingerprinting applications for authentication purposed to curb the problem of digital piracy.

We amplify generalizing so as to exist plans the entrance tree to a benefit tree. we amplify generalizing so as to exist plans the entrance tree to a benefit tree. The key purpose of the character data spillage we had in our past plan and additionally every current property based encryption plans is that key generator issues Attribute key in light of the reported trait, and the generator needs to know the client's ascribe to do as such[3].

II. Proposed Solution Analysis & Design

Proposed Solution Analysis

Property based encryption is utilizing information transferred. This is every last hub scrambled information in store. Fine-Grain idea utilizing encoded information change over into twofold esteem completely secure for database. Different procedures have been proposed to secure the information substance protection through access control. we propose AnonyControl and AnonyControl-F to permit cloud servers to control clients' entrance benefits without knowing their character data[4][5].

They will take after our proposed convention when all is said in done, yet attempt to discover however much data as could reasonably be expected separately. The proposed plans can secure client's protection against every single power. Fractional data is revealed in AnonyControl and no data is uncovered in AnonyControl-F. We firstly execute the genuine toolbox of a multi authority based encryption plan AnonyControl and AnonyControl-F[12].

Registration -Based Social Authentication

The framework gets ready trustees for a client Alice in this stage. In particular, Alice is initially confirmed with her fundamental authenticator (i.e., password),and then a few companions, who additionally have accounts in the framework, are chosen by either Alice herself or the administration supplier from Alice's companion list and are designated as Alice's Registration[6][7][11].

• **Security**

Validation is vital for securing your record and keeping caricature messages from harming your online notoriety. Envision a phishing email being sent from your mail since somebody had produced your data. Irate beneficiaries and spam grumblings coming about because of it turn into your chaos to tidy up, with a specific end goal to repair your notoriety. trustee-based social confirmation frameworks request that clients select their own trustees with no requirement. In our investigations, we demonstrate that the administration supplier can oblige trustee determinations by means of forcing that no clients are chosen as trustees by an excess of different clients, which can accomplish better security ensures.

Attribute- based encryption

Property based encryption module is utilizing for every last hub scramble information store. After encoded information and again the re-scrambled the same information is utilizing for fine-grain idea utilizing client information transferred. the trait based encryption have been proposed to secure the distributed storage. Attribute Based Encryption (ABE). In such encryption plot, a personality is seen as an arrangement of expressive traits, and decoding is conceivable if a decrypter's character has a few covers with the one determined in the ciphertext.

Multi-authority

A multi-power framework is displayed in which every client has an id and they can

 ISSN: 2454-4248
500 – 509

associate with every key generator (power) utilizing diverse nom de plumes. We will probably accomplish a multi-power CP-ABE which accomplishes the security characterized above; insurances the privacy of Data Consumers' personality data; and endures bargain assaults on the powers or the conspiracy assaults by the powers. This is the primary execution of a multi-power quality based encryption plan.

Proposed Algorithmic Solution

If Z were to be modeled as Gaussian distributed, the joint maximum-likelihood (ML) estimator of V and decoder of B would be:

$$\hat{,}\hat{} = \arg\min_{z1/2} (Y - VB)_{2f} \ldots\ldots\ldots(1)$$

$$B \in \{\pm 1\}^{k \times m}$$

$$V \in {}^{L \times K}$$

where multiplication by $z1/2$ can be interpreted as prewhitening of the compound observation data. If Gaussianity of Z is not to be invoked, then (1) can be simply referred to as the joint generalized least-squares (GLS) solution(2Generalized least-squares solutions are weighted least-squares (WLS)solutions with optimal weighting matrices, here $z1/2$ that yield the lowest variance of the estimation error) of V and B.

The global GLS -optimal message matrix $\hat{}$ in (1) can be computed independently of$\hat{}$ by exhaustive search over all possible choices under the criterion function

$$z1/2\,(Y - VB)_{2f}\,\hat{=} \arg\min_{z1/2} (Y - VB)_{2f} \ldots\ldots\ldots(2)$$

$$B \in \{\pm 1\}^{k \times m}$$

$$V \in R^{L \times K}$$

where $P_{\perp B} = I - B^{T}(BB^{T})^{-1}B$.

The derivation of (2) Exhaustive search has, of course, complexity exponential in KM (total size of hidden messages in bits). We consider this cost unacceptable and attempt to reach a quality approximation of the solution of (2) (or (1), to that respect) by alternating generalized least-squares estimates of V and B, iteratively, as described below. Pretend B is known. The generalized least-squares estimate of V is

$$\hat{}_{GLS} \arg\min_{z1/2} (Y - VB)_{2f} \ldots\ldots\ldots(3)$$

$$V \in R^{L \times K} = YB^{T}(BB^{T})^{-1}$$

(3) Pretend, in turn, that V is known. Then, the least-squares estimate of B over the real field is

$$\hat{}_{GLS\ real} = \arg\min_{z1/2} (Y - VB)_{2f} \ldots\ldots\ldots(4)$$

$$B \in R^{K \times M} = (V^{T} R_{z\text{-}1} V)^{-1} V^{T} R_{z\text{-}1} Y.$$

(4) Observing that $(V^{T} R_{z\text{-}1} V)^{-1} V^{T} R_{z\text{-}1} = (V^{T} R_{z\text{-}1} V)^{-1} V^{T} R_{y\text{-}1} \ldots\ldots\ldots(5)$,

(5) we rewrite

$$\hat{}_{GLS} (V^{T} R_{z\text{-}1} V)^{-1} V^{T} R_{z\text{-}1} \mathbf{Y}$$

and suggest the approximate binary message solution Bb

$$\hat{}_{GLS} = \min_{z1/2} (Y - VB)_{2f} \ldots\ldots\ldots(6)$$

$$V \in R^{L \times K} = YB^{T}(BB^{T})^{-1}$$

(6) The proofs of (3), (4), and (5) are provided in the Appendix. The multi-carrier iterative generalized least-squares (MIGLS) procedure suggested by the two equations (3) and (6) is now straightforward. Initialize Bb arbitrarily and alternate iteratively between (3) and (6) to obtain at each step conditionally generalized least squares estimates of one matrix parameter given the other. Stop when convergence is observed. Notice that (6) utilizes knowledge of the autocorrelation matrix Ry, which can be estimated by sample averaging over the received data observations, $_{y} = 1\,\Sigma$.

The M-IGLS extraction algorithm is summarized in Table I. Superscripts denote iteration index. The computational complexity of each iteration of the M-IGLS algorithm is O(2K3+2LMK +K2 (3L+M)+L 2K) and, experimentally, the number of iterations executed is between 20 and 50 in general. For the sake of mathematical accuracy, we recall that in least-squares there is always a symbol sign (phase in complex domains) ambiguity when joint data extraction and carrier estimation is pursued (i.e., data bits bk ∈ {±1}M on carrier sk ∈ R L have the same least-squares error with data bits −bk on carrier −sk, k = 1, . . . , K). The sign-ambiguity problem can be overcome with a few known or guessed data symbols for supervised sign correction3 . Moreover, in a multi-carrier least-squares scenario as the one that we face herein, the index association remains unresolved (i.e., given a recovered (message, carrier) pair (b, s), the corresponding index k ∈ {1 , K} in (1) cannot be obtained).

TABLE I MULTI-CARRIER ITERATIVE GENERALIZED LEAST-SQUARES DATA EXTRACTION

 ISSN: 2454-4248
500 – 509

1) d := 0; initialize Bb (0) ∈ {±1}K×M arbitrarily.

2) d := d + 1;

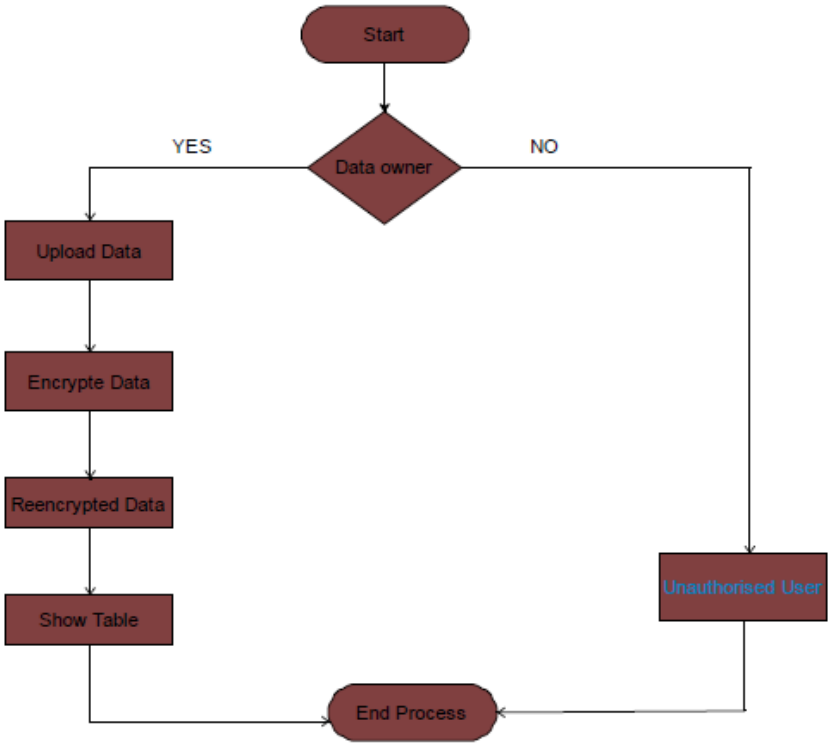
$\hat{}_{(d)} = Y(B_{(d-1)})^{T} (B_{(d-1)}) (B_{(d-1)})^{T}$]

$\hat{}_{(d)} = sgn ((V (d))^{T} {}_{-1} y (Vb (d)) -1 (Vb (d))^{T}$ Rb −1 y Y .

3) Repeat Step 2 until Bb (d) = Bb (d−1) .

Extend that the application of the work presented in this paper is to simply extract blindly the embedded bits with the least possible errors, the carrier indexing problem is not dealt with any further. Returning to the proposed data extraction algorithm, we understand that with arbitrary initialization convergence of the M-IGLS procedure described in Table I to the optimal GLS solution of (9) is not guaranteed in general. Extensive experimentation with the algorithm in Table I indicates that, for suf- ficiently long messages hidden by each carrier (M = 4Kbits or more, for example), satisfactory quality message decisions Bb can be directly obtained. However, when the message size is small, M-IGLS may very well converge to inappropriate points/solutions. The quality (generalized-least-squares fit) of the end convergence point depends heavily on the initialization point and arbitrary initialization -which at first sight is unavoidable for blind data extraction- offers little assurance that the iterative scheme will lead us to appropriate, "reliable" (close to minimal generalized least-squares fit) solutions. To that respect, re-initialization and re-execution of the M-IGLS procedure, say P times, is always possible. To assess which of the P returned solutions, say (Vb 1, Bb 1), . . . ,(Vb P , Bb P), has superior generalized-least-squares fit, we simply feed (Vb i , Bbi) to (9) (using Rb y in place of Rz) and choose Vb final, Bb final = arg min (V,B)∈{(Vb 1,Bb 1),(Vb P ,Bb P)} kRb − 1 2 y (Y − VB)k 2 F . (16) The computational complexity of the P-times re-initialized MIGLS is, of course, O(P D(2K3 + 2LMK + K2 (3L + M)+ L 2K)) where D represents the number of internal iterations in d in Table I .

Data flow process



 ISSN: 2454-4248
500 – 509

Solution Implementation

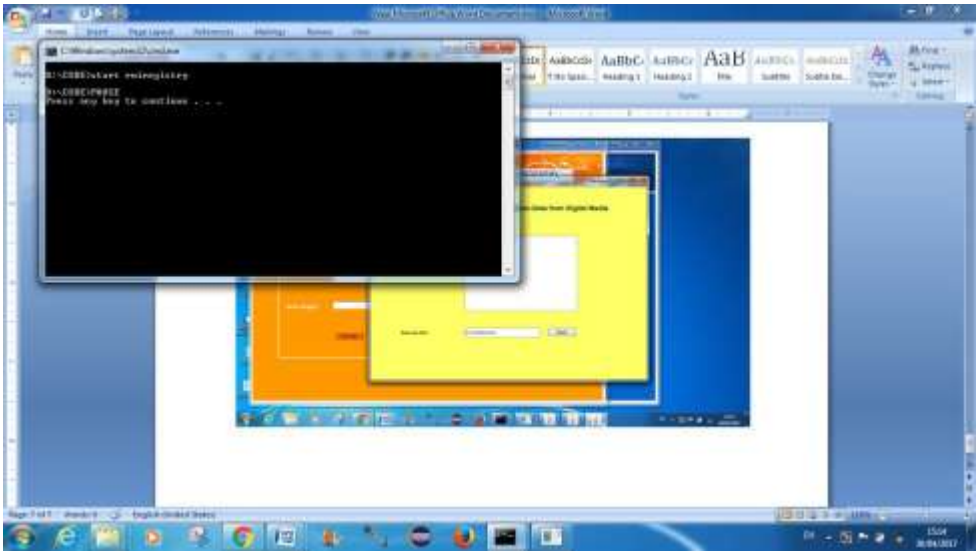
As far as the computer is concerned, an image is just a 2-D array of pixels. The color of each pixel is encoded an integer between 0 and 16.8 million (2_{24} - 1 to be precise), with 8 bits dedicated to each of the red, green, and blue primaries. Flipping the ones bit of this number (i.e. subtracting 1 from an odd number or adding 1 to an even number) changes the amount of blue in the color by a minute amount that is indistinguishable to the human eye.

Hiding information: As we discussed in class, image steganography will represent the information to be hidden as a sequence of bits, and then hide that sequence of bits in the image. We will assume the information to be hidden is made up of (English) letters, digits, and punctuation marks, represented as bits according to the ASCII character set[8].

Then, we will simply set the least significant bit (LSB) of each successive pixel to 0 or 1 to match the values of each bit in your message. This will cause the blue value of each pixel to change by at most one step, which won't be noticeable; but now each pixel in the image carries one bit of your message. Since ASCII requires 7 bits to represent a single character, each character of your message will be spread across 7 pixels in the image[9][10].

Execution is the phase of the venture when the hypothetical outline is transformed out into a working framework. Hence it can be thought to be the most basic stage in accomplishing a fruitful new framework and in giving the client, certainty that the new framework will work and be compelling. The usage stage includes watchful arranging, examination of the current framework and it's requirements on execution, planning of systems to accomplish changeover and assessment of changeover techniques.

Interfaces to implement



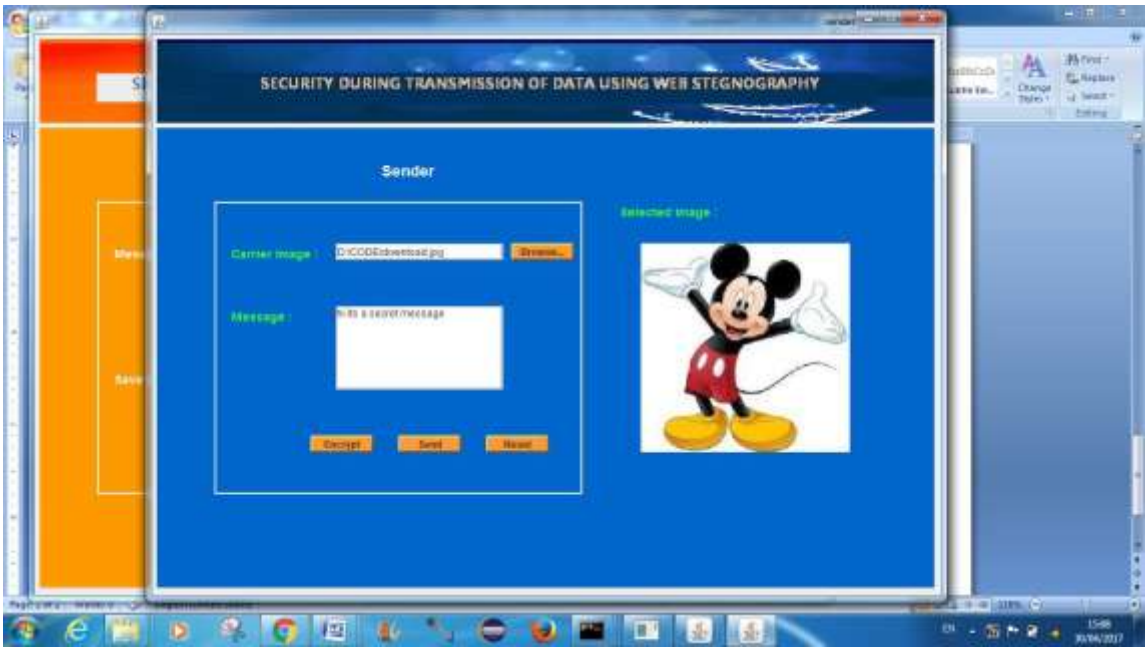
Screen – 1: Sender screen

 ISSN: 2454-4248
500 – 509

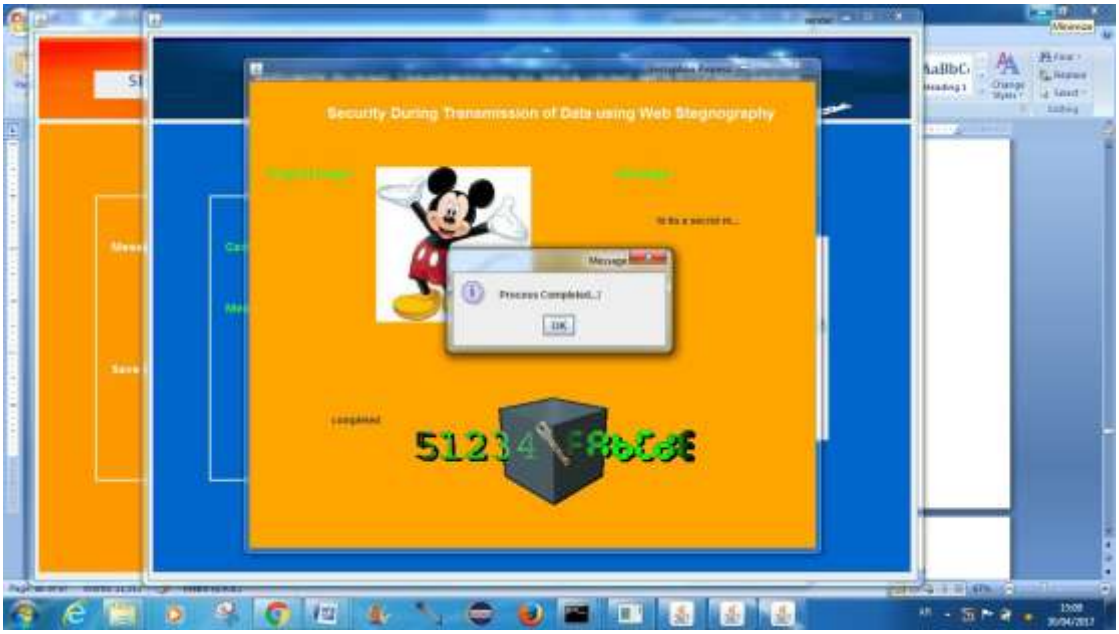
Screen – 2: Sender authentication

Screen – 3: Conversion of data into image

 ISSN: 2454-4248
500 – 509



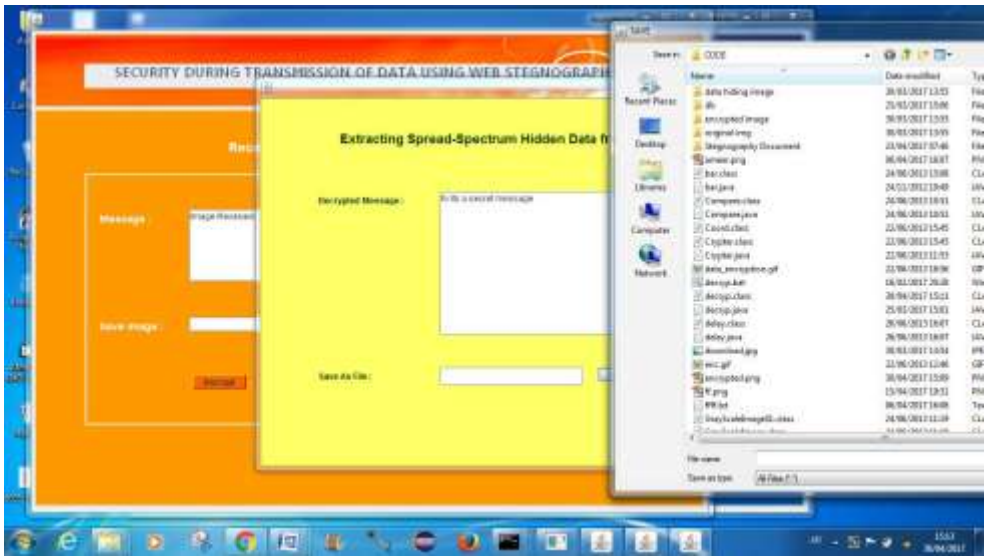
Screen – 4: After adding the image for transmission



Screen – 5: Successfully encrypted data with image

ISSN: 2454-4248
500 – 509

Screen -6: Recipient authentication



Screen -7: Decrypting the encrypted file with authenticated code

 ISSN: 2454-4248
500 – 509

I V. Conclusion

This paper proposes a semi-mysterious property based benefit control plan AnonyControl and a completely unknown trait based benefit control plan AnonyControl-F to address the client protection issue in a distributed storage server. Utilizing different powers as a part of the distributed computing framework, our proposed plans accomplish fine-grained benefit control as well as personality namelessness while directing benefit control in view of clients' character data. All the more critically, our framework can endure up to N − 2 power trade off, which is profoundly best particularly in Internet-based distributed computing environment. We additionally led itemized security and execution investigation which demonstrates that Anony-Control both secure and productive for distributed storage framework. The AnonyControl-F straightforwardly acquires the security of the AnonyControl and along these lines is comparably secure as it, however additional correspondence overhead is caused amid the 1-out-of-n negligent exchange.

One of the promising future works is to present the proficient client denial system on top of our mysterious ABE. Supporting client denial is a vital issue in the genuine application, and this is efficient test in the utilization of ABE plans. Making our plans good with existing ABE plans who support productive client disavowal is one of our future works.

IV. References

1. Bitar, N., Gringeri, S., & Xia, T. J. (2013). Technologies and protocols for data center and cloud networking. Communications Magazine, IEEE, 51(9), 24-31.
2. Houidi, I., Mechtri, M., Louati, W., & Zeghlache, D. (2011, July). Cloud service delivery across multiple cloud platforms. In Services Computing (SCC), 2011 IEEE International Conference on (pp. 741-742). IEEE.
3. Nurmi, D., Wolski, R., Grzegorczyk, C., Obertelli, G., Soman, S., Youseff, L., & Zagorodnov, D. (2009, May). The eucalyptus open-source cloud-computing system. In Cluster Computing and the Grid, 2009. CCGRID'09. 9th IEEE/ACM International Symposium on (pp. 124-131). IEEE.
4. Okuhara, M., Shiozaki, T., & Suzuki, T. (2010). Security architecture for cloud computing. Fujitsu Sci. Tech. J, 46(4), 397-402.
5. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.
6. Ramgovind, S., Eloff, M. M., & Smith, E. (2010, August). The management of security in cloud computing. In Information Security for South Africa (ISSA), 2010 (pp. 1-7). IEEE.
7. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.
8. M. Barni, F. Bartolini, and T. Furon, “A general framework for robust watermarking security,” ACM Journal Signal Proc. - Special Section: Security of Data Hiding Technologies, vol. 83, pp. 2069-2084, Oct. 2003.
9. S. Lyu and H. Farid, “Steganalysis using higher-order image statistics,” IEEE Trans. Inform. Forensics and Security, vol. 1, pp. 111-119, Mar. 2006.
10. G. Gul and F. Kurugollu, “SVD-based universal spatial domain image steganalysis,” IEEE Trans. Inform. Forensics and Security, vol. 5, pp. 349-353, June 2010.
11. Y. Wang and P. Moulin, “Steganalysis of block-DCT image steganography,” in Proc. IEEE Workshop on Statistical Signal Processing, SaintLouis, MO, Sept. 2003, pp. 339-342.
12. A. Valizadeh and Z. J. Wang, “Correlation-and-bit-aware spread spectrum embedding for data hiding,” IEEE Trans. Inform. Forensics and Security, vol. 6 , pp. 267-282, June 2011.