International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Preserve the Confidentiality of Information in E-government Through Steganography Based on AES technique and Unicode Standard

Abdulrahman Ahmed Alzand[1], Omar Hisham Rished[2]

[1]Programmer / Ministry of Science and Technology, Iraq

[2]Assistant lecturer / Iraqi University, Iraq

Abstract: ***Government basically alludes to give proficient, advantageous and transparent services to residents and business through data and communication technology. Governance is an option structure to the conventional perspective of government. One of the fundamental tasks of e-government is the transmission of private data from conventional to computerize on the PC systems. Albeit every e-government has its own systems and government can't deny utilizing Internet. In any case, to ensure data is prime worry for e-government and secure them with the web assaults since Internet is making a borderless world. Data security implies ensuring data and data frameworks from unapproved get to, utilize, revelation, interruption, alteration, scrutiny, investigation, recording or demolition. Data security is a set joining authoritative security and IT security. This paper concentrates on the most proficient method to secure data utilizing steganography. As steganography is solid information concealing strategy, by utilizing it is extremely helpful to shroud information as well as accommodating in character get to administration. The strategy is created to conceal the secret information with the specific picture. It is useful in security of data, exactness and straightforwardness among subjects. The paper additionally concentrates on the provisos of other information concealing method called cryptography. As data security is a prime worry in online world, it pulls in light of a legitimate concern for scientists to grow new systems and consistent assessment of it.***

Keywords: Cryptography, Advance encryption standard(AES), Steganography, Unicode Standard

1. Introduction

One reason that interlopers can be effective is the large portion of the data they obtain from a framework is in a shape that they can read and grasp. Interlopers may uncover the data to others, change it to distort an individual or association, or utilize it to dispatch an assault. One answer for this issue is, using Steganography. Steganography is a strategy of concealing data in advanced media. As opposed to cryptography, it is not to shield others from knowing the shrouded data however it is to shield others from believing that the data even exists. Steganography turn out to be more critical as more individuals join the internet transformation. Steganography is the craft of disguising data in ways that keeps the recognition of shrouded messages[1]. Steganography incorporate a variety of mystery specialized strategies that conceal the message from being seen or found. Because of advances in ICT, a large portion of data is kept electronically. Thus, the security of data has turned into a crucial issue. Other than cryptography, Steganography can be utilized to secure data. In cryptography, the message or scrambled message is implanted in an advanced host before going it through the system; accordingly the presence of the message is obscure. Other than concealing information for secrecy, this approach of data stowing away can be reached out to copyright assurance for advanced media: sound, video and pictures. The developing potential outcomes of present day interchanges require the unique methods for security particularly on PC arrange. The system security is ending up noticeably more critical as the quantity of information being traded on the web increments[2], Thusly, the secrecy and information respectability are requires to ensure against unapproved get to and utilize. This has brought about an unstable development of the field of data concealing Information covering up is a rising exploration zone, which incorporates applications, for example, copyright assurance for advanced media, watermarking, fingerprinting, and Steganography. Steganography shroud the emit message inside the host informational collection and nearness vague and is to be dependably imparted to a collector. The host informational collection is deliberately adulterated, yet clandestinely, outlined to be imperceptible to a data analysis.

2. What is Steganography?

Steganography is the act of hiding private or delicate data inside something that has all the earmarks of being nothing out to the standard thing. Steganography is regularly mistaken for cryptology on the grounds that the two are comparable in the way that they both are utilized to secure critical data. The contrast between two is that Steganography includes hiding data so it creates the impression that no data is hiding by any stretch of the imagination. On the off chance that a man or people see the protest that the data is hiding within he or she will have no clue that there is any hiding data, accordingly the individual won't attempt to decode the data [3].What Steganography basically does is misuse human perception, human faculties are not prepared to search for documents that have data within them, and despite the fact that this product is accessible that can do what is called Steganography. The most well-known utilization of Steganography is to conceal a record inside another document.Throughout history Steganography has been used to secretly communicate information between people.

Assaults on Steganography Techniques:

1) Visual Attacks: Visual Attacks are generally viewed as the most straightforward type of steganalysis. As the name recommends, a visual assault generally includes analysing the subject record with the bare eye to recognize the distinction.
2) Auxiliary Attacks: Structural assaults are intended to exploit the abnormal state properties of the structure of the bearer.
3) Factual assault: In arithmetic, the investigation of measurements makes it conceivable to decide if some Phenomenon happens aimlessly inside an informational collection.

Project Scope:
This paper is developed for hiding information in any documents file. The scope of the paper is implementation of Steganography tools with AES techniqueand Unicode Standard for hiding information includes any type of information file and documents files inside the server to protect this documents in E-government servers.

Methodology:
User needs to run the application. The user has two tab options – encrypt and decode. If user select encrypt, application give the screen to select document file, information file and option to save the document file. If user select decode, application gives the screen to select only document file and ask path where user want to save the secrete file. This project has two methods – Encrypt and decode.

- In encryption the secret information is hiding in with any type of document file.
- Using AEStechniqueto keep the information more secret and difficult to steal
- Decoding is getting the secret information from document file.

3. Related Work

There are numerous viewpoints to security and numerous applications. One basic perspective for secure interchanges is that of cryptography. Cryptography is system for keeping message secure and free from assaults. In cryptography mystery message is mixed. Cryptography is the investigation of scientific systems identified with parts of data security, for example, privacy, information honesty, substance validation, and information starting point confirmation [2]. Correspondence security of information can be expert by methods for standard symmetric key cryptography. Such imperative information can be dealt with as double grouping and the entire information can be encoded utilizing a cryptosystem. It has been numerous years research to encryption innovation, there are numerous encryption calculations. The three sorts of calculations are portrayed:

- Symmetric Algorithm or Private Key Uses a solitary key for both encryption and decoding.
- Asymmetric or open key Algorithm Uses one key for encryption and another for decoding
- Hash Functions: Uses a scientific change to irreversibly "encode" data.

Steganography is the other procedure for secured correspondence [3]. Steganography includes covering up data so it gives the idea that no data is covered up by any means. On the off chance that a man or people sees the question that the data is covered up within he or she will have no clue that there is any concealed data, along these lines the individual won't endeavor to unscramble the data. Steganography is the procedure of concealing a mystery message inside cover medium for example, picture, video, content, sound [9].

Picture steganography has numerous applications, particularly in the present current, cutting edge world. Security and mystery is a worry for a great many people on the web. Picture steganography takes into account two gatherings to impart subtly and secretively. It takes into account some ethically cognizant individuals to securely shriek blow on interior activities; it permits for copyright insurance on. One of the other primary uses for picture steganography is for the transportation of abnormal state or, on the other hand top-mystery records between global governments Steganography frameworks can be gathered by the sort of covers utilized (sound, content, executable) or by the strategies used to alter the spreads.

- Substitution framework
- Transform space strategies
- Spread range methods
- Statistical strategy
- Distortion methods

A. Advanced Encryption Standard:
Propelled Encryption Standard is the Rijndael calculation by two specialists Dr. Joan Daemon and Dr. Vincent Rijmen from Belgium [10], [11]. Not at all like its ancestor, DES, AES does not utilize a Feistel organize [12]. The AES calculation is a symmetric key square figure with a piece length of 128 bits and support for key lengths of 128, 192, and 256 bits. The AES calculation is a symmetric key calculation which implies a similar key is utilized to both scramble and decode a message. Likewise, the figure content created by the AES calculation is an indistinguishable size from the plain instant message. A large portion of the operations in the AES calculation happen on bytes of information or on expressions of information 4 bytes in length, which are spoken to in the field GF (28), called the Galois Field. AES depends on an outline standard known as a Substitution change organizes. AES works on a 4×4 grid of bytes, named the state. The AES figure is determined as various reiterations of change adjust that change over the info plaintext into the last yield of cipher text. Each round comprises of a few handling steps, including one that relies upon the encryption key. An arrangement of turn around rounds is connected to change cipher text once again into the first plaintext utilizing a similar encryption key. The AES calculation circles through specific areas Nr times. It is quick in both programming and equipment.

B. Unicode Standard
The Unicode Standard is the all-inclusive character encoding plan for composed characters and content. It characterizes a reliable method for encoding multilingual content that empowers the trading of content information universally and makes the establishment for worldwide software [13].

Unicode can be actualized by various character encodings. The most normally utilized encodings are UTF-8, UTF-16. UTF-8 utilizes one byte for any ASCII characters, which have similar code esteems in both UTF-8 and ASCII encoding, and up to four bytes for different characters. UCS-2 utilizes a 16-bit code unit (two 8-bit bytes) for each character[14]. Unicode characters are recognized by code focuses, which are expectedly spoken to by the letter U took after by four or five hexadecimal digits, for instance U+00AE or U+1D310. Unicode characters can go in scalar esteems from 0 to over a million. The whole scope of Unicode characters is isolated into 17 obstructs, each square is alluded to as a plane and is numbered beginning from 0. Characters in the Basic Multilingual Plane (BMP), containing present day contents – including numerous Chinese and Japanese characters – and numerous images have a 4-digit code. Notable contents, yet in addition numerous advanced images and pictographs, (for example, emesis, numerous CJK characters, and Egyptian Hieroglyphics) have 5-digit codes [13]. At that point, Unicode allude to the group of models and advancements related with the Unicode Consortium that can be used for working with a composed dialect in a PC environment [14].

Mix Algorithm (AES + Unicode) has following steps.

1) Open cover document.
   AES Algorithm has following steps.
2) Key Expansion—Round keys are gotten from the figure key utilizing Rijndael's key calendar.
3) Initial Round
   - A - Add Round Key—every bite of the state is joined with the round key utilizing bitwise XOR.
4) Rounds
   - Sub Bytes—a non-direct substitution step where each byte is supplanted with another as indicated by a query table.
   - Shift Rows— a transposition step where each line of the state is moved consistently a specific number of steps.
   - Mix Columns—a blending operation which works on the sections of the state, joining the four bytes in each section.
   - Add Round Key
5) Final Round (no Mix Columns)
   - Sub Bytes
   - Shift Rows
   - Add Round Key Points of interest of utilizing AES calculation
   a) Very Secure.
   b) Reasonable Cost.
   c) Main Characteristics
   i) Flexibility, ii) Simplicity

Unicode Algorithm has following steps.

6) Find selected characters in Table 1.
7) Compute number of selected characters to check the capacity of hiding.
8) Get binary form of secret message.
9) For each two symbol in secret message - if bit = 00, then no change (ASCII code), else replace by Unicode of Multilingual characters in Table 1.
10) Return stego document.

4. Proposed System

In this paper, a new method was presented for text steganography in English scripts using Unicode of multilingual characters with AES, the target of the proposed conspire is to plan high security show for security of mystery information. In this period of widespread electronic network, of infections and programmers, of electronic listening in and electronic misrepresentation, there is to be sure a need to shield data from going before inquisitive eyes or, all the more vitally, from falling into wrong hands. To secure data against security breaks and assaults there is need of more complex strategies of ensuring mystery information. To dodge the issue of unapproved information get to steganography alongside cryptography is the privilege generally arrangement. In proposed framework cryptographic and steganography security is consolidated to give two level securities to mystery information. To begin with imperative message is scrambled by utilizing advance encoded standard (AES) encryption calculation. A piece graph of proposed framework for information implanting is appeared in Figure 1.

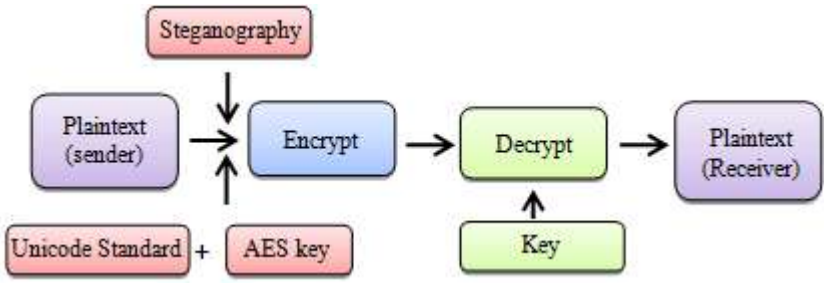

Figure 1: Proposed Message Embedding Procedure

In Unicode, two procedures were executed, concealing procedure, and extricating process. Concealing procedure in view of the presence of chose characters in English content. In this strategy two bits can insert at one time. Right off the bat chose characters must to be found in record, at that point installing process executed by substitution relying upon mystery message which can be covered up. Also, substitution should be possible in view of mystery message.

Hiding process (Embedding process) summarized in the following algorithm:

EmbedAlgorithmhas following steps.
Input of info: Encrypted Secret Data (D), Cover Image(C)
Output: Stego image(S) with mystery information implanted in it.

1) Divide scrambled mystery information into three Data pieces D1,D2, D3.
2) Convert the every Secret Data pieces (D1, D2, and D3) into paired configuration.
3) Split the cover picture C into Red, Green and Blue.(R,G and B individually)
4) Divide Red (R) cover picture into non covering pieces of two back to back pixels.
5) Call AES with Unicode calculation to insert encoded mystery information piece D1 into Red (R) of cover picture.
6) Call AES with Unicode to insert encoded mystery information piece D2 into Blue (B) of cover picture.
7) Call AES with Unicode calculation to insert encoded mystery information piece D3 into Green (G) of cover picture
8) Find selected characters in Table 1,
9) Compute number of selected characters to check the capacity of hiding.
10) Get binary form of secret message.
11) For each two symbol in secret message - if bit = 00, then no change (ASCII code) else replace by Unicode of Multilingual characters in Table 1.
12) Hide the message length in the beginning of secret message.
13) Store the subsequent picture as Stego Image (S) Block chart of proposed framework for information extraction is appeared in Figure1

Through the algorithm above, divide the algorithm into three pieces (d1, d2, d3) and then convert each piece of pieces(D1, D2, D3) to the associated configuration and then divide the cover image into red, green and blue (R, B, G)Individually, and then call the common algorithm (AES + Unicode) to insert the codec (D1) intoRed (R) of the cover image and so have the call individually for the rest of the basic colors (B, G) with the algorithm(AES + Unicode) and added to (D2, D3), then search for the characters specified in table 1 and calculate the specified characters are checked for the ability to hide so as to obtain the binary form of the confidential message through the text where if the text = 00 does not change within (ASCII) and then hides the text inside the envelope as seen from Figure 1.

5. Results

In this paper, the proposed method is chosen by taking different documents of different sizes and hiding the data of the e-government within the envelope. As seen in the GUI corresponding to the method suggested in Figure 3.

Figure 2: GUI interface System

In this system the designer include the image in all extensions with the text that is also all extensions and when clicking the word encryption will do the algorithm for this project and the conversion of data inside the casing as shown in Figure 3

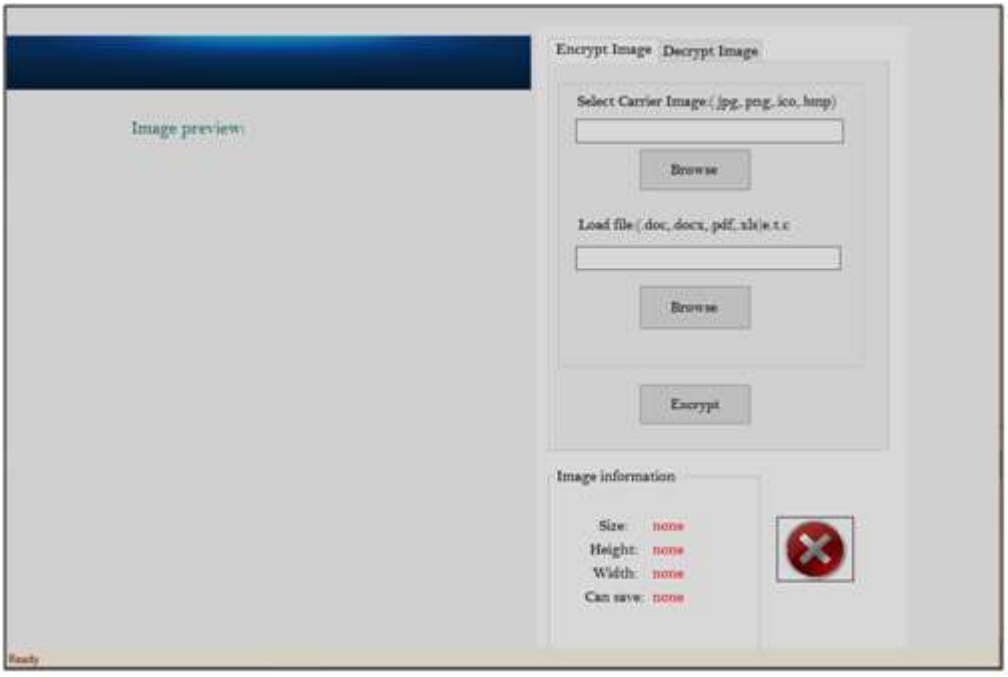

Figure 3: GUI of proposed method

As we see in Figure 4, the data may be embedded in the image where the data was contained in the Word file and the program gave the message a successful embedding and did not change the colour and image format.

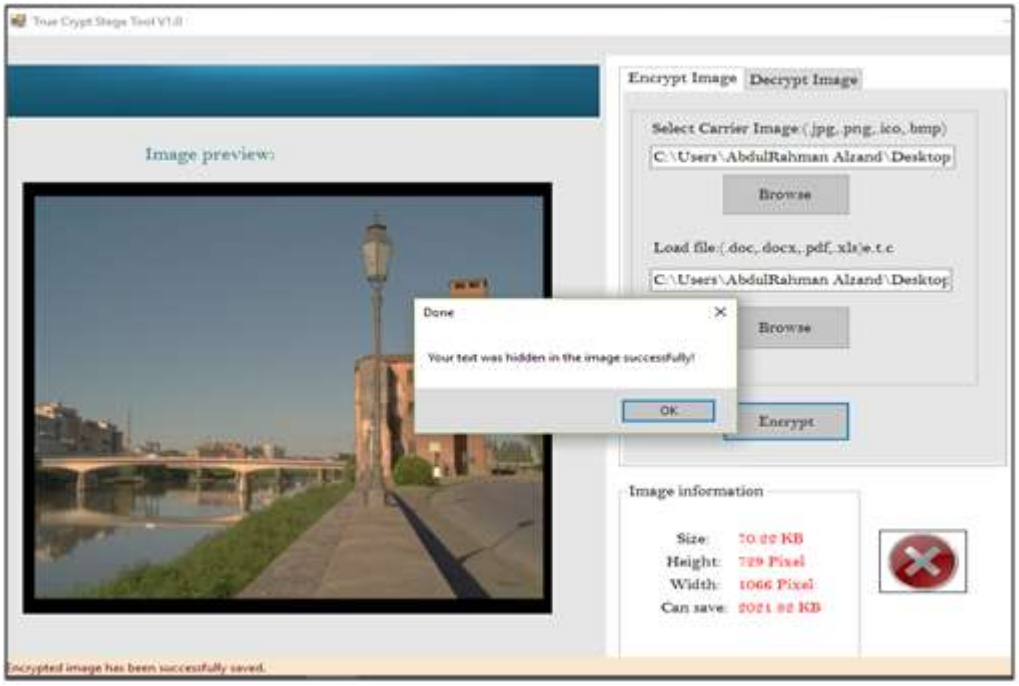

Figure 4: Stego images Created by our approach (embedded data are 2021.82 KB)

6. Conclusion

Security is vital for proficient communications. Cryptography and steganography are two noteworthy branches of information security. In this proposed framework cryptographic and steganography security is joined to give two level securities to mystery information. In proposed conspire mystery message is scrambled before concealing it into the cover picture which gives high security to mystery information. Propelled encryption standard (AES) is utilized to encode mystery Message and Unicode substitution strategy is utilized to stow away scrambled mystery message into cover picture. Proposed approach majors in more critical advancement in the terms of flexibility, limit, and imperceptivity. Trial comes about demonstrate that proposed approach acquires both bigger limit and higher picture quality. it's a nice practice to shroud information it helps in getting character administration and what's more information security is accomplished by it. This framework is profitable to check the data likewise by exploiting it we can lessen the hazard and secure information and exact flawlessness. At long last we can infer that the proposed procedure is viable for mystery information correspondence.

References

[1] United Nations, Department of Economic and Social Affairs (2012). "E-Government Survey 2012.E-Government for the People".ISBN:978-92-1- 123190-8.
[2] J. Boritz, Efrim (2011). "IS Practitioners' Views on Core Concepts of Information Integrity".International Journal of Accounting Information Systems.Elsevier.
[3] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker (2007). "Digital Watermarking and Steganography (Second Edition)", Morgan Kaufmann Publishers.
[4] B. Schneier (2004). The Nonsecurity of Secrecy. Communications of the ACM,47(10), 120-120. Retrieved August 2, 2008, from Academic Search Premier database.
[5] M.Baker,(2005). Keeping a Secret. Technology Review, 108(1), 82-83. Retrieved August 12, 2014, from Academic Search Premier database.
[6] S.Robinson (2008). Safe and secure: data encryption for embedded s ystems. (Coverstory). EDN Europe, 53(6), 24-33. Retrieved August 2, 2008, from Academic SearchPremier database.
[7] A. Kerckhos (1883). La Cryptographie Militaire. "Journal des Sciences Militaries, vol. 9, pp. 538.
[8] B. P Fitzmann (1996). "Trials of traced traitors." Information hiding, first international work shop, Lecture notes in computer science R. Anderson, Ed. Berlin, Germany: Springer Verlag 1996, vol. 1, pp= 49-64.
[9] M. D. Swanson, B-zhu and A. H. Tewfik, (1996). "Robust Data Hiding for Images" in proc. IEEE Digital signal processing workshop, Loen, Norway,pp-37-40.
[10] Joan Daemen, Vincent Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard." in Springer, 2002 ,ISBN 3-540- 42580-2.
[11] Christof Paar, Jan Pelzl, "The Advanced Encryption Standard" Textbook for Students and Practitioners.
[12] Data Encryption Standard (DES)'.National Bureau of Standards (US).Federal Information Processing Standards Publication National Technical Information Service. Springfield VA. April 1997.
[13] J. Korpela, *Unicode explained* (United States of America., O'Reilly Media , 2006).
[14] D. Yacob, Unicode for Under-Resourced Languages, 2006, 33-38. From http://mt-archive.info/LREC-2006-Jacob.pdf

Table 1: Selected English alphabets for hiding process

Symbols	*ASCII*	*Unicode*		
	Secret message 00	*Secret message 01*	*Secret message 10*	*Secret message 11*
A	0041	0391	0410	13AA
B	0042	0392	0412	0181
E	0045	0395	0415	13AC
G	0047	050C	13C0	13B3
H	0048	0397	041D	13BB
I	0049	0399	04C0	0406
M	004D	039C	041C	216F
O	004F	039F	041E	0555
P	0050	0420	03A1	01A4
S	0053	0405	054F	13DA
T	0054	0422	03A4	01AC
J	006A	0458	03F3	029D
O	006F	03BF	1D0F	043E