Asian Journal of Convergence in Technology *Volume II Issue III*
Issn No.:2350-1146, I.F-2.71

Ancient and Modern Steganography

Saugata Dutta
Research Scholar, OPJS University,
Churu, Rajasthan, India

Dr. Om Prakash
OPJS University,
Churu, Rajasthan, India

Abstract: **Steganography is an art of putting information in a medium without causing significant and statistically difference in the medium. The word steganography conjoins words "steganos" which means covert and "graphein" meaning writing, which means hidden writing. Steganography is although not a new art and had been used during the ancient times. The steganography process has changed from ancient times to digital age but the concept remained the same. This paper will discuss on various methods used during ancient times and evolution and used in recent times.**

Keywords—Steganography, Cryptography, Microdots, Wax Tablet.

I. INTRODUCTION

Steganography as the name suggest means cover writing [1]. It is actually concealing or hiding information in different mediums such that the information can be passed without any suspects and can be transferred from the sender end to the receiving end. Steganography being used from ancient times and was the one of the best art to transfer information from receiving end to the closing end. In recent era, the concept remained the same but the technique has changed with the advancement of new technology and constant development in every aspects of life. In recent years life is driven by technology so as the changes in different hiding techniques. One should not confuse with steganography and cryptography.

As steganography is an ancient art, the modern formulation comes from the prisoner's problem as proposed by Simmons [2], where it states that there are two prisoners named Alice and Bob who wish to exchange secret information through a warden named Eve. The information shared will be hidden and will be exchanged which gives the birth of steganography. Eve will give punishment if she suspects any type of secret information. The warden on the other hand can inspect the medium and material of communication. There are two wardens active and passive. The active warden will modify the information if suspected and passive warden will note the information and inform several people and pass on the information. So hence we can understand that any secret information is passed from a sender to a receiver through any medium and accessed without notice of others is an art of steganography based on this model. The solution is to create a sublime channel.

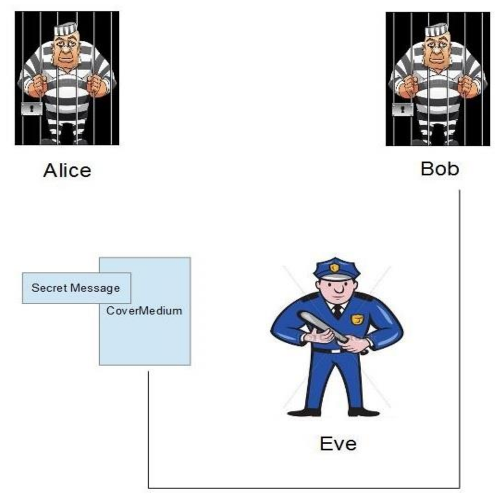


Fig. 1. Prisoners Problem

Steganalysis on the other hand is an art of detecting the hidden information. The main objective of steganography is to break the steganography and detect the hidden data. There are two methods one is statistical steganalysis and the other is feature based steganalysis. There are various tools for steganalysis such as StegDetect, StegSecret, JPSeek, StegBreak etc.

In Modern age there are different types of steganography like text, image audio and video

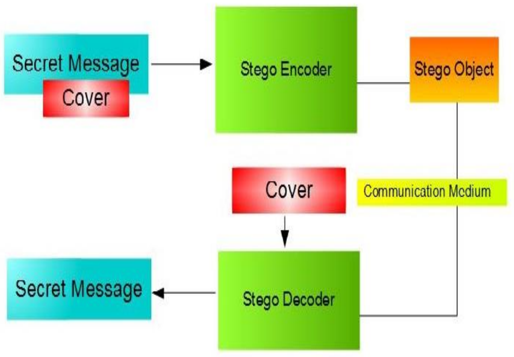


Fig. 2. Basic steganography process

broadly. The most common tools for steganography are Outguess, OpenStego, Xiao, Silent eye, SteganPEG etc. There are broadly two methods of steganography techniques which is spatial domain which can be further classified into LSB Technique, Pixel Value Differencing and Pixel Indicator. While the other is Transform domain which can also be further classified into Discrete Cosine Transform and Discrete wavelet transform.

This paper discuss about the evolution of steganography from the ancient era to modern age. The paper throws light on the techniques of steganography used during the ancient times and transformation of techniques in the modern digital age.

II. REVIEW LETREATURE

Manisha Saini and Gaurav Saini explored tools being used for primarily data hiding and encryption. There are some common tools being used for Images, audio and video files. It also shows the virtual disk to be hidden in WAV (Audio) files. StegFs which is a steganographic file system for Linux. Spam Mimic is a popular steganographic tool that allows user to hide information in SPAM messages [3].

Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt explored the emerging techniques DCT (Discrete Cosine Transform), DWT (Discrete Wave Transform) and adaptive steganography are not to prone to attacks, especially when the message is small. This is because they alter the coefficients in the transform domain, thus image distortion kept to minimum. Generally these methods tend to have a lower payload compared to spatial domain algorithms [4].

Navneet Kaur and Sunny Behal surveyed wide variety of techniques used in steganography like Least Significant Bit, Discrete Cosine Transform and Discrete Wavelet Transform which helps to improve security [5].

Youssef Bassil et al. (2011 proposed a new steganography method for text hiding. It revolves around using two mediums to transmit secret textual data from sender to receiver. The first medium is a user defined pangram English text sentence made up of a maximum of 512 characters including letters, digits and special characters. The second medium is a digital uncompressed image file mainly a BMP type image [6].

Dr. Mahesh Kumar and Munesh Yadav et al. (2014): developed a method for image steganography using frequency domain. In this method major importance is given on the secrecy as well as the privacy of the information, where DWT operations provide sufficient secrecy [7].

Mehdi Hussain and Mureed Hussain analysed different proposed techniques which show that visual quality of the image is degraded when hidden data increased up to certain limit using LSB based method and also many of them embedding techniques can be broken or shows indication of alteration of image by careful analysis of the statistical properties of noise or perceptually analysis [8].

Ms. Anshu Sharma and Dr. Deepti Sharma proposed a system where it used LSB Technique for embedding the Text message and the three techniques i.e. AES, DES and Blow fish for encrypting and Decrypting the Information before sending it to the client. This showed how various techniques can be combined to provide more security by combining cryptography with steganographic techniques [9].

James C. Judge explored steganography in multiple forms which has been used literally for thousands of years. It showed that the most effective use of steganography has been used effectively during the time of war or civil strife. Location of some forms of steganographic content would require techniques other than statistical profiling not the least of which could be visual examination [10].

Z. V. Patel and S. A. Gadhiya explored the overview of image steganography, cryptography, its uses and techniques. It also attempts to identify and briefly reflects on which steganographic techniques are more suitable for which applications [11].

Yao Lu et al. (2014) explored a method to detect audio steganography by using combination of forensic tools but also proposes a forensic guideline from the experience gained from the research testing in in investigating audio steganography [12].

III. ANCIENT STEGANOGRAPHY

As stated earlier that steganography started during the ancient era. In back to the primeval times Caesar took the pride of inventing Caesar cipher around 50 B.C. to foil his communication from being examined. Histaiacus during the 6 Century BC used to shave the head of messenger and wrote a note asking Aristagoras of Miletus to revolt against the king pf Persia. Once the messenger’s hair grew back, the messenger was dispatched with the message. The other form of hiding message during the ancient times is writing message over the silk and cover compressed to make a ball. The ball is then covered with wax and then the ball is swallowed by the messenger. These are actually the examples of human vectors.

The Geoglyphs are the greatest examples for a certain form of steganography. The Nazca lines in Peru, the Uffington White Horse 1 in England, Cerne Abbas Giant in England, Paracas Candelabra in Peru, and the Atacama Giant in Chile are some giant figures which can only be viewed from the air.

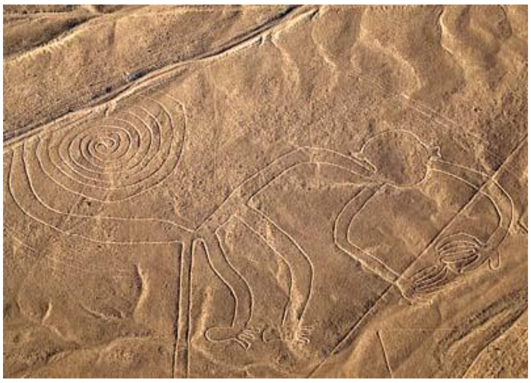


Fig. 3. Nazca Lines in Peru, Geoglyphs [13]

In 480 BC, Demaratus sent a message to the Spartans warning a possible war Xerxes by writing on a wooden backing of a wax tablet and then covering the same with beeswax.

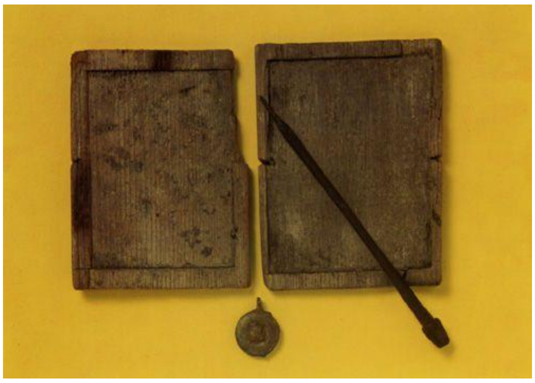


Fig. 4. Ancient Wax Tablet

Mary Queen of scots used to hide letters inside the bunghole of a beer barrel which used to freely pass in and out of the prison. Steganographia, which was written in 1499 by Johannes Trithemius and was not published until 1606. The name of the book meant concealed or covert writing and various techniques in hiding messages over different medium being outlined. The first two parts were book on concealed writing techniques and the third part was more on occult astrology.

Tacitus invented a method the Astragalus which is the predecessor for today’s cubical die. A set of Astragali could be used to conceal a message by means of weaving a thread through the holes in a pre-determined manner. Such object would actually pass as a toy.

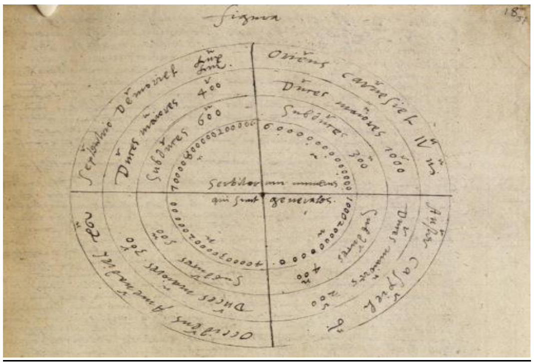
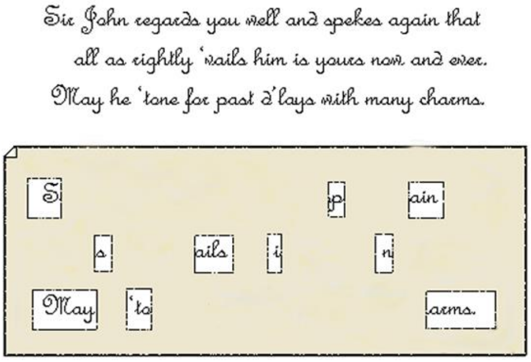


Fig. 6. A Chart from Steganographia [14]

Girolamo Cardano invented a method of hiding text using a grid. A Cardan Grille was a sheet of parchment with apertures of writing text. A text in the holes formed the steganogram which was composed into innocent looking text. When the grill is laid over the printed text, the intended message can be retrieved.



Sir John regards you well and spekes again that
all as rightly 'wails him is yours now and ever.
May he 'tone for past d'lays with many charms.

Fig. 7. Cardan Grille [15]

In more recent history during the period of World Wars several types of steganography methods were used like microdots, invisible ink and sign language.

During the World War II, used microdots to send information back and forth. Microdots are small minute that is basically half the size of the period produced by the type writer. Microdots needs to be embedded in the paper and covered with an adhesive. This was reflective and thus detectable by viewing against glancing light, alternatively inserting microdots into slits cut into the edge of the postcards. These dots could contain the pages of information, drawings etc.

Using of secret inks or rather invisible ink on paper under other messages or on the blank parts of other messages.

During the World War II, a spy for japan, Velvalee Dickinson sent information to America. She was a dealer in doll and her letters discussed some information about the dolls. The stego text was the doll orders and the concealed text was the information on movement of the ships etc. She became famous and she was known to be the doll woman.

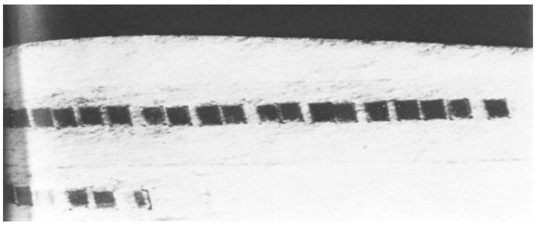


Fig. 8. Microdots during the World War

In 1968, crew members of the USS Pueblo, intelligent ship held as prisoners by North Korea communicated in sign language during staged photography, informing the United States that they were held captive.

There were evidences before civil war the way to provide information to slaves for their escapes by using various patterns in quilts which were commonly hung from windowsills to dry, messages were passed to slaves guiding them in their quest. The example of such is Bear Paw Symbol advised to follow the bear tracks over the mountain.

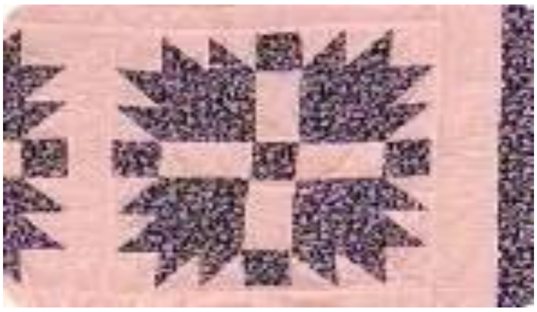


Fig. 9. Bear Paw Symbol [10]

IV. MODERN STEGENOGRAPHY

In Modern era, the use and technology of steganography is totally different from the one being used in the olden days. Now is the time of digital life, the informations are hidden inside text, image, audio and video files. There are majorly five types of steganography which is Text steganography, Image Steganography, Audio steganography, Video steganography and Protocol steganography.

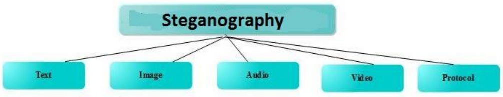


Fig. 10. Modern Steganographic Techniques

In text steganography, the approaches are hiding by selection, HTML documents, Line and Word shifting, hiding using white spaces, semantic based hiding, and abbreviation based hiding. Hiding by selection is the way by selecting the character in the cover text and embed the data. HTML Tags can be used to hide the data in an HTML documents. Line and Word shifting vertically and horizontally respectively can be used as a covert writing. White spaces can also be used in text steganography where two white spaces implies 1 is hidden and one space is 0. So based on this terminology, the receiver retrieves the data. In semantic based hiding, synonyms of word being used. In abbreviation based hiding, a lexical dictionary is created with corresponding abbreviation and then replace the carrier text with this abbreviation. Text steganography using digital files is not used very often, the reason is the text files have a very small amount of redundant data.

Image steganography is said to be the most common form of digital steganography. Here a secret message is embedded in the digital image with an embedding algorithm with using a secret key which is optional. A key when used is said to be using steganography with cryptography. The cover medium is said to be the image file. The image file is then transmitted to the receiver through a public network precisely internet. The image cover file is then decoded with a decoding algorithm and the secret message is retrieved. The general public can only notice the image but can’t guess the existence of the secret message. The cover images used in the image steganography are jpeg, bmp, gif, png etc. where out of these jpeg provides the maximum compression ratio with good image quality. Hence jpeg format is being used in current trends in image steganography. There are various tools for steganography like QuickStego, OpenStego, StegonG, Hide n Reveal, StegoShare, SteganPEG etc.

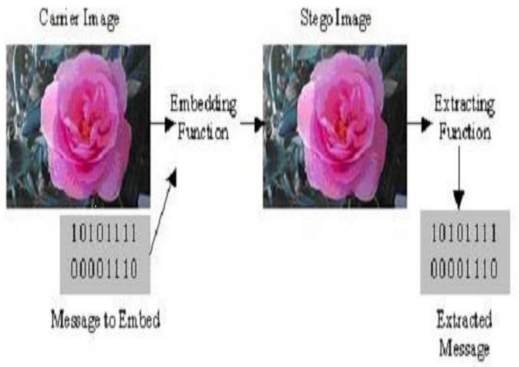


Fig. 11. Image Steganography [16]

Audio steganography on the other hand is hiding secret message in an audio file with commonly mp3 and wav format as cover file. It exploits the virtue of human ear to hide information unnoticeably. An audible sound cannot be heard in presence of another loud audible sound. This property actually allows to select the channel to hide the information. The main attributes of audio steganography are sampling rate, amplification, adding noise, quantization, encoding and decoding, filtering and transcoding. The secret message can be hidden in the form of echo which is known as echo hiding. There are some drawbacks in audio steganography like in a wav file format as a medium up to 500 characters can be embedded, increase amount of secret data may cause complexity, estimable interface, more time in computation, frequency discrepancies etc. Some of the audio steganography tools are SilentEye, Xiao, DeepSound, Clotho etc.

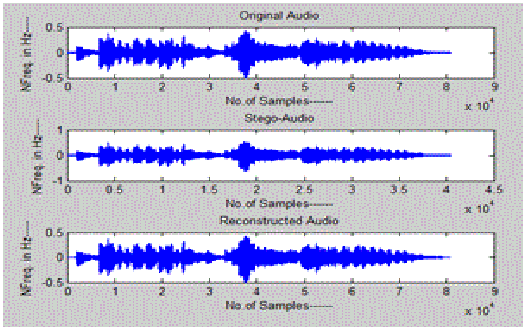


Fig. 12. Audio Steganography [17]

Since video is basically a combination of image and audio, their steganographic techniques are pertinent to video as well. Instead of transferring image and audio separately, the video is transferred from sender to receiver. Secret message in video steganography can be a text, audio or image. This application is developed for embedding secrets in an inoffensive medium. Unlike others, key is optional component in video steganography. The huge benefits for using video steganography is to embed more data in comparison to audio steganography and the distortion goes unnoticed as video is contagious flow of data. The algorithm is more complex as compared to other steganographic techniques and this resists attacks. Some of the video steganography tools are Camouflage, OpenPuff, RT Steganography, Stegosaurus etc.

The process in which the secret message or text is embedded in a network protocol it is known to be protocol steganography. This is also a form of private communication. The most common example is embedding data in TCP/IP header and the other way is manipulating the TCP/IP packet length. Another example is embedding data in SIP protocol that is in VOIP communication. In spite of rigorous experiments, linguistic verification, statistical test, protocol steganography is said to be more secured and great means of communication. Some of the tools are StegoSIP and SteganRTP while there are many more.

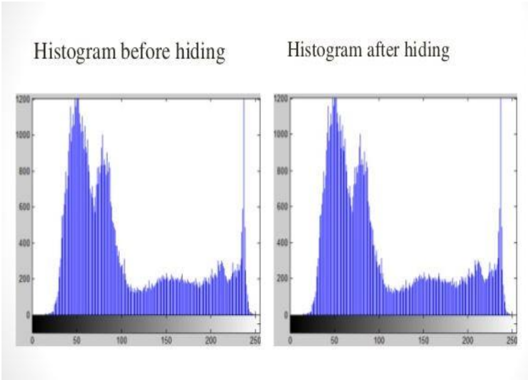


Fig. 13. Video Steganography [18]

V. STEGANALYSIS

Steganalysis is a process in which the secret data can be detected and retrieved from the suspected stego file. The only way this can be achieved is to put the right algorithm on the stego cover file. There are various types of attacks in steganography.
Stego-Only Attack where the cover file is analyzed and only applicable techniques are applied to detect the secret data. Known Cover Attack is a technique where both cover and stego object is compared and differences are compared. Known Message Attack is a techniques in which known secret message and sample stego image is analyzed where the same protocol is used to retrieve the hidden message from the stego object. In Chosen Stego Attack the hidden information is known with respect to the stego object and the steganographic tools to extract it. Chosen Message Attack checks the matching pattern of the generated stego object and can determine the particular steganographic algorithm. Known Stego Attack in which verification of actual and stego object is done using steganographic algorithm. There are several tools for steganalysis like Jsteg-shell, JPhide, and Outguess 0.13b, Invisible Secrets, F5, appendX, Camouflage, Hiderman, JPHIde and Seek, Masker, JPegX. Steganography analyser real-time scanner which can analyse the network traffic in real time and provide the steganographic communication details.

VI. USE OF MODERN STEGANOGRAPHY

There are various advantages and disadvantages of steganography. The main advantage of using steganography is Digital Watermarking. It is used to protect a copyright material by embedding a digital sign, signature, hologram or text on top of the image, video or audio. The digital signature is not always visible or may not be identified as it becomes a part of the image. In 2010 scientists at Georgia Tech had created a method of communication by means of popular photo sharing sites like Picassa or Flickr [19]. In 2011 researcher from Tufts University has found some evidences to hide with the help of bacteria possessing fluorescent capabilities. Steganography can be used for securing data in a better manner.

The disadvantages are more as it said to be more used in hiding information and used in terrorism. The terrorist attack on 9/11 said to have used steganography in some major location to share files [19]. The second issue of technical magazine for jihadi has used some images where secret messages were crafted. There were news way back in 2004 that some printer manufacturers hides tracking information in print outs. There are certain facts from different parts of the world that some spy agencies use steganography technology to upload images or videos to transport embedded secret messages. Malwares uses steganography to send data or get control over the system. In operation Shady RAT in 2011, information where smuggled in crafted HTML and jpeg files. The Duqu Worm in 2011 took control over some system centers with the help of image files. Some multiplayer games are used for steganography communication. Private chat rooms in games are suspected to be used in covert communication similar in Xbox and PlayStation.

VII. CONCLUSION

Steganographic communication is not a new art. The concept remains the same but the time, medium and technology changes. Starting from ancient times to the modern age, this art is being used. In modern age, steganography is being exploited in terrorism and seems to be in use of its darkest side. The prospective future of steganography is increasing day by day which can be more vibrant and can be used for noble cause. It is indeed an interesting way of communication as there are less complexity in implementation.

ACKNOWLEDGEMENTS

I am thankful to my project guide who has supported me enormously in the experiment and also my sincere thanks to professors and friends for the encouragement.

REFERENCES

[1] http://en.wikipedia.org/wiki/Steganography

[2] Gustavus, J. Simmons., "The Prisoners' Problem and the Subliminal Channel", in Proceedings of CRYPTO '83, pp 51-67. Plenum Press (1984).
.

[3] Saini, Manisha. and Saini, Gaurav., "Steganography and tools used for steganography", *International journal of scientific and engineering research*, January 2014, pp. 1693-1697.

[4] Cheddad, Abbas., Condell, Joan., Curran, Kevin., and Kevitt, Mc. Paul., "Digital image steganography: Survey and analysis of current methods", *Signal Processing*, 2010, pp. 727-752.

[5] Kaur, Navneet., and Behal, Sunny., "A Survey on various types of steganography and analysis of hiding techniques", *International journal of engineering trends and technology*, May 2014, pp. 388-392.

[6] Bassil, Youssef. (2012). A Text Steganography Method using pangram and image mediums. International Journal of Scientific and Engineering research. 3 (2).

[7] Kumar, Mahesh. and Yadav, Munesh., (2014). Image Steganography Using Frequency Domain. International Journal of Scientific & Technology Research. 3 (9). 226-230

[8] Hussain, Mehdi. and Hussain, Mureed., "A Survey of Image Steganography Techniques", International Journal of Advance Science and Technology, May 2013.

[9] Sharma, Anshu., and Sharma, Deepti., "Research on Analysis of Different Image Steganography Techniques", *International Journal of Engineering Sciences and Research Technology*, June 2014, pp. 570-577.

[10] Judge, C. James., "Steganography: Past", Present, Future *Sans Institute*, 2001.

[11] Patel, V. Z., and Gadhiya, A. S., "A Survey paper on Steganography and cryptography", International multidisciplinary Research Journal, May 2015.

[12] Lu, Yao. (2014). Investigating Steganography in Audio Stream for Network Forensic Investigations: Detection and Extraction, Master of Forensic Information Technology, AUT University, Auckland, New Zealand.

[13] http://www.unmuseum.org/nazca.htm

[14] https://en.wikipedia.org/wiki/Johannes_Trithemius

[15] https://en.wikipedia.org/wiki/Cardan_grille

[16] http://www.freeprojectscode.com/java-projects/image-steganography/2158/

[17] http://www.yuvaengineers.com/decimated-wavelet-with-spread-spectrum-approach-for-audio-steganography-b-venkata-ramana-naik-p-s-s-sumapriya/

[18] http://www.slideshare.net/ShajanaKBasheer/video-steganography-46652967

[19] http://stegano.net/tutorial/steg-history.html