International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 6 Issue: 4 267 - 277

Web Service Deployment for Selecting a Right Steganography Scheme for Optimizing Both the Capacity and the Detectable Distortion

R. Pavithra
PG Scholar,
Department of IT,
P.S.V. College, Krishnagiri, India

R.Srinivasan
Head of the Department,
Department of IT,
P.S.V. College, Krishnagiri, India

V.Saravanan
Assistant Professor,
Department of IT,
P.S.V. College, Krishnagiri, India

ABSTRACT: The principal objective of this effort is to organize a network facility to hide the secret information in an image folder without disturbing its originality. In the literature lot of algorithms are there to hide the information in an image file but most of it consumes high resource for completing the task which is not suitable for light weight mobile devices. Few basic algorithms like 1LSB, 2LSB and 3LSB methods in the literature are suitable for mobile devices since the computational complexity is very low. But, these methods either lack in maintaining the originality of the source image or in increasing the number of bits to be fixed. Furthermore, every algorithm in the literature has its own merits and demerits and we cannot predict which algorithm is best or worst since, based on the parameters such as size of the safety duplicate and encryption algorithm used to generate the cipher text the steganography schemes may produce best or worst result with respect to computational complexity, capacity, and detectable distortion.

In our proposed work, we have developed a web service that takes cover image and plain text as the input from the clients and returns the steganoimage to the clients. The steganoimage will be generated by our proposed work by analyzing the above said parameters and by applying the right steganography scheme. The proposed work helps in reducing the detectable distortion, computational complexity of the client device, and in increasing the capacity. The experimental result says that, the proposed system performs better than the legacy schemes with respect to capacity, computational complexity, and detectable distortion. This proposed work is more useful to the client devices with very low computational resource since all the computational tasks are deployed in the server side.

*****

1. Introduction

Steganography is mainly focused on hiding of asecret communication withinaregular communication and the abstraction of it at its purpose. Steganography can be used along cryptography a footstep by hiding a coded message so that no one respondents it occurs. Preferably, if someone scan your data will fail to know it contains codeddata. The systems can be functional to images, a video file or an audio file that can be an extra-secure method in which to protect data. Steganography can be used for top-secret communications that contract with terroristplans Data can be stolen and encrypted through a file transfer or in many way through email. In ancient Greece, a message would be written on a wooden panel and then covered in wax. These and other methods of hiding communications are nothing compared to what we can do today with the advent of computer technology. It is now so much easier to hide information and so much harder to detect it.

Steganography defends from exciting copyrighted materials as well as aiding in unauthorized viewing. It must be encrypted, which can be nearly impossible. As an industry we are moving towards the encryption of data on our laptops and desktops and through our computer security policies we block the writing of data to our USB devices, any employee can use the corporate network to send out anything they wish through email. Many companies employ a type of email monitoring which scans the email for key expressions to try to detect if someone is sending out knowledgeable property other companies will block the sending of word or excel documents and allow only PDF documents to be sent out.This prevents fake actions and gives copyright protected media secured filed with extra protection.

Steganography code is an art of hiding one communication in additionalmissive, here it's the art of hiding text in the image. Data Safety is becoming an extremely significant part of Information Communication. Steganography is datasecurity ariskystatementnetwork is one of the most challenging issues. Cryptography and steganography, a punishment of data hiding, are two different popular security offering methods.Security organizationscontain both cryptography and steganography in their working code. To handle up with those systems, we have proposed a format-based pure text steganography system including a private key cryptography providing a higher level of security.

The protectionscript has been made as normal as imaginable. After successful embedding of the secret note into the protectionscript, the stego-text also looks like an ordinary text because only an alphanumeric puzzle is added at the end of the cover text to make up the stego-text.Increasing the growth of the communication segments the higher level of security of data has become one of the basic needs for transmitting information over the unsecured

communication channel. Information Safety is attractive an extremely important part of Data Statement.The resultant compactednote is further compressed using the Huffman lossless compression technique. Finally, the compressed underground communication is embedded into the protectionbased on the modulus three of the difference between DCT coefficients of the cover image during JPEG compression process.

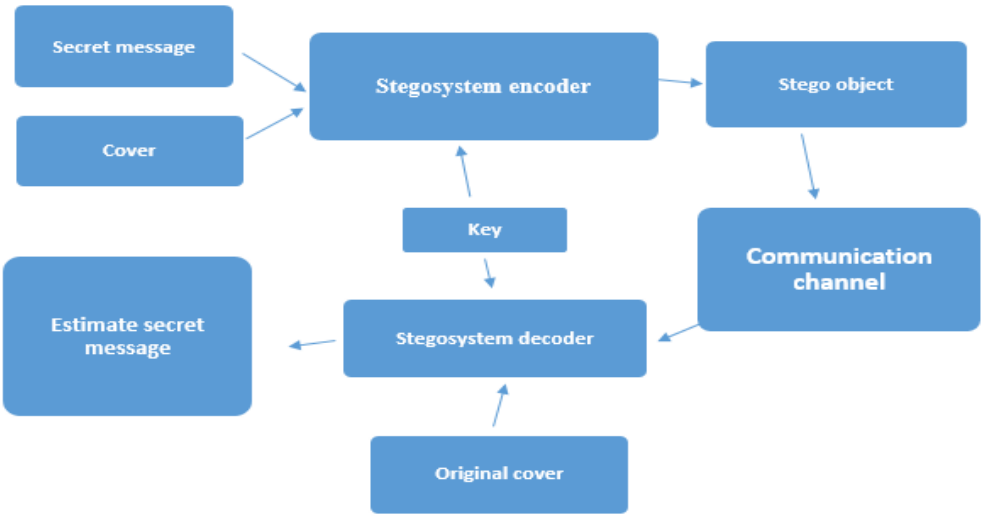

Figure 1.1 Basic working principles of steganography

The increasingopportunities of current communication requirement the special means of safety especially on computer network. Datasafety in the last few years has expanded a extensivespectators. The effectiveness of the proposed method is described pictorially and also has been shown that a multi-level of security of data can be achieved.The main goal of steganography is to communicatemessage securely in a complete undetectable mannerDigital technology gives us a new way to relate steganographic techniques including hiding information in digital images. It not only goes well beyond simply by embedding a text in an image, but also pertains to other media, including voice, text,binary files and communication channels.

The problem of unauthorized copying now-a-days is of great concern especially to the music, film, book and software publishing industries. To overcome such type of problems, some invisible information can be embedded in a digital media in such a way that it could not easily be extracted without any specialized techniqueIn the other side to it, cryptography is one of effective solution to protect the data from the unauthorized users. It can be mentioned here that although by the use of cryptographic techniques we can convert the data into a cipher text, which is in unreadable format, we can not hide the existence of the same data. Therefore, cryptography in alone is not sufficient to protect the data against the unauthorized access by unauthorized users if they can not hide their significantdata, this may lead to damage extremely the company's effectiveness as well as its sustainability.

When by means of a 24-bit image, one bit of each of the major color workings can be used for the above resolution. It can be seen that on an normal only a half of the bits in an image will need to be improved to hide a secret message using the maximum protectionscope.

Advantages of Steganography

- Steganography is advantageous for hiding messages for transmission
- Steganography is main parous of securing data
- Steganography is a advantageous technique for securely storing sensitive data
- Hiding coordination passwords or keys within other files.
- Assume i have hide a secret message inside an image, it will look normal to normal eye it won't position out.
- We use steganography to hide cryptography.
- Steganography is the secret communications that deal with terrorist plans Data can be taken and codedconcluded a file transfer or in many way through email.
- These are the advantages of Steganography systems
- The steganography is for protecting the data, such as in the field of media where the copywriting safeguards the verification.
- The steganography can be used by the intellect supports for communicating their secret information

Disadvantages/limitations of steganography

- By using the steganography tool many terrorist and have anti-humanist activities have happened.
- Message stands solid to recuperate if duplicate is subject to attack such as transformation and replacement
- Importantdamage to photograph presence message difficult to recuperate.
- Comparatively easy to notice, as our development has exposed.
- If the size of the original file is already known or estimated then that could be a potential threat to the excess of the memory that it would show in its properties
- If the decrypting JavaScript has been exploited or destroyed or meddled with then the information that had been sent could be safely considered as lost or irrevocable

If the passphrase for the steganography usefulness as in the stegohide value for Linux based platform is conceded or misplaced or overlooked then again removal of the hidden contented would be nearly difficult. Steganography finding can be used to avoidstatement of nasty data.The LSB addition system is the most common and easiest method for implanting messages in an image with high capacity. But the limitation of this is the secret message is easily detectable The proposed method combines samples of LSB bits by using addition modulo to form the value which is compared to the part of the secret message. If these two values are equal, no change is made. Otherwise, add the difference of these two values to the sample. Thus, this future method implantations the part of the secret communication effectively. Numerical analysis is performed on stego image created using the steganography method.

The main control is the extreme size of the rooted data associated to the total data. If a piece of data is already very compressed it might be wholly impossible to embed additional data in it. And even under ideal conditions you will rarely get more than 20% out of the carrier data.I assume of course that the data hidden is encrypted first, making it appear completely random even to statistical analysis programs. This reduces those (ideal) 30% by half on average.So assume that you use a bunch of image files of moderate compression level as carrier medium. Let's say you get on average 15% out of it, say the total batch of images has a size of 1GB.This means that after encrypting and embedding your data, you will be able to transport 75MB of hidden datathis is not a lot.

Steganography is in general only used in situations where there is no other alternative because the very fact that A and B are communicating would lead to grave consequences. Trying to swap and share files for example is not such a situation.

2. Literature Survey

Most of the persons anxious about the security of confidential information because Confidentiality is an energetic part Sensitive information should be confidential because data can be accessed by intruders. Secrecy of message has always been a challenging task. For securing our communication, we use several types of steganography techniques. Steganography is the most popular technique to hide the data from intruders and none other than observer can recognizes the existence of content. The existence of content cannot be presumed out by the smart reader. Steganography is the technique by which we can share sensitive information surreptitiously and securely

The quantity of confidential information inserted would be like that it does not diminish the excellence of stego-image there are several types of SteganographyThe technique should be the volume of sensitive message that can be inserted without distortion of the quality of the image (capacity) and even to the receiver the grade of effort, necessary to alteration of inserted information deprived of destroying the frontidentical.

This method includes physical alteration of the format of text to hide the information. But if stego-file is opened by using word processor, spelling errors and unusable tabs will get detected. Different font's sizes can stimulate doubt to a clever reader. Stenographic typescript would make operated portions of typescript quite observable. One of the most significant techniques of steganography can embed the confidential information in the image. This is achieved by adjusting the pixels values. Severalfootings that are limited in Image Steganography

- Cover Image: An importer of confidential information.
- Stego Image: When secret information is embedded into the mask image, the resulting image is known as stego image.
- Message: The original data which is to be concealed.
- Stego key: To embed and retrieve the original data through surrounding and retrieving algorithm respectively, the stego key is required.

There are number of techniques that can be employed in image steganography which are as follows

- Digital multimedia data provides a robust and easy editing and modifying of data. The data can be delivered over computer
- Networks with little to no errors and often without interference. Unfortunately, digital media distribution raises a concern for digital

- Content owners. Numerical data can be imitatively lacking any loss in superiority and content. This poses a big problem for the protection of
- Intellectual property rights of copyright owners. Watermarking is a solution to the problem. It can be defined as embedding digital
- Data, such as information about the owner, recipient, and access level, without being detectable in the host multimedia data.
- Steganography relies on hiding covert message in unsuspected multimedia data and is generally used in secret communication
- Between acknowledged parties. Steganography is a method of encryption that rawhides data among the bits of a cover file, such as a
- Graphic or an audio file. The technique replaces unused or insignificant bits with the secret data. Steganography is not as robust to
- Attacks since the embedded data is vulnerable to destruction. Watermarking has the feature of robustness against attacks. Even if the
- Existence and method of embedding the data is known, it may be difficult to destroy the hidden data. Data hiding and data

Embedding can be classified as methods between steganography and be watermarking.

- Text steganography
- Image steganography
- Audio steganography
- Video steganography
- TCP/IP packets

As discussed in [2], today everyone uses computer networks and Internet to share resources and to exchange information between the connected nodes. This computer network on based the properties like practice, topology and architecture. Based on the needed security level, cost factor, performance and implementation limits any one of this type can be used. Topology defines the bodily preparations of the lumps of a network. Widely known topologies are bus, ring, star, mesh and hybrid. In the bus topology, all the nodes will be connected using a single cable (this cable will act as a backbone). Damaging the cable will cause network failure. The information can be easily hacked by hackers by taping the cable anywhere in the network. This is a simple and cheap topology to implement. In-ring topology the nodes of a network will connect via a ring-like a cable. Comparing bus topology it is good for speed and information can be hacked easily by taping the cable.

In a star topology, the network devices like hub or switch will be used to connect all the nodes of a network. Tapping of the single cable may not be used to hack all the data of all the nodes if the network uses switches because switch simply forwards the frame to a specific port, which is connected to a specific node of the network. In case if a network uses the hub, then taping a single cable is enough to monitor or hack the data into a network. Many hacking, network monitoring and packet capturing tools are available in the market. This will break the security in both wired and wireless networks. Mesh topology connects all the nodes of a network to each other. It is expensive because it needs a number of cables and network adapters. Here the advantage is a failure of the single cable may not affect the network performance and the network will be more stable. During the information exchange, the data will travel in multiple paths, so hacking is tough than previous topologies.

Using architecture also we can classify the networks. Widely known architectures are peer-to-peer and client-server. In peer-to-peer, all nodes can communicate with each other without any specific server node to control. It is suitable for small companies or institutions where the number of nodes is less. Generally, this type of architecture used to share resources like storage capacity, internet, printers, scanners and other things. Most of the small companies and DTP canters use this type of network for easy installation.

In a client-server architecture, a specific node can act as an NT Domain Controller, which controls all the nodes of a network. All the nodes can log in to the server to get a specific service. During the login process, the nodes have to send the username, password and other information like text by captcha for proper authentication. The client-server architecture is good in case of security comparing peer-to-peer. Because of security reasons many big companies use this type of architecture. Also, the security risk is very high in wireless networks than wired networks, since the signal spreads over the air, the hackers can sit anywhere in the coverage area to hack the data.

In wireless networks, the communications happen with electromagnetic signals. These signals need no line of sight like infra-red communication. This electromagnetic signal will spread in all the directions and anyone can receive the signals by sitting anywhere in the network's coverage area. Thus we cannot able to provide physical security for the communication medium and providing security is tough in a wireless network than a wired network. The nodes of the wireless networks are mobile in nature. The mobile node has many limitations comparing fixed nodes [1-4]. They are

- ❖ Low Computing Power
- ❖ Low Memory
- ❖ Limited Power Backup
- ❖ Low Connectivity Speed

Because of the above mentioned limitations, the security algorithm or schemes developed for fixed nodes may not be suitable for the mobile nodes [8], [9]. Hence, a

special care has to be taken while developing new algorithm or scheme related to security or other purpose.

Generally video compression techniques will reduce the redundancy in video data to reduce the size of the video file. Maximumaudio-visualfirmnessprocesses and code uses both three-dimensional image compression and progressivesignaladvantagemethodscollected. Also, most video code uses audio compression systems together to compress the audio streams. The highly compressed video may present visible or distraction artefacts. Sequence of still images called frames may form a video data. Each frame is made up of number of pixels. The sequence of frames contains both spatial and temporal redundancy that video compression systems try to make it in smaller dimension. If one frame contains areas, where nothing has changed comparing previous frame then, the system simply issues a short command to copy that part from the previous frame. If a group of frames have small changes comparing each other, then the system simply issues a command that tells the de-compressor to rotate, lighten, darken or shift the copy (This command is little longer than the previous case but shorter than the intrafirm compression). The interface technique is good in case the video is just played by the user, but when try to edit the video, problem will occur, because interface compression makes the player to copy, the following frames cannot be reconstructed properly during editing process.

Some video formats such as DV uses intrafirm compression, making video editing easy. In the format like MPEG2 (That uses interface compression), certain frames are there called "I-Frame", which may not allowed to copy data from other fames and requires more data than nearby fames. Rate control plays a vital role in high quality video encoding. Achieving the perceptual quality at a given bit rate through the proper bit allocation process is the main goal. Using the frame other frame types like P-Frame, B-Frame and D-Frame along with I-Frame, the Bit rate of the video can be adjusted as needed.

As said in [11] the nodes in a peer-to-peer network will communicate with one another. The information exchanged by these nodes can be easily hacked by using any one or more of the hacking tools such as IP Sniffer (Build around packet sniffer), Nagios (The Open Source Network Monitoring Software), MRTG (The Open Source Traffic Monitoring Software), REMSTATS (Network monitoring software), Symons (Network monitoring software), Cricket (Router monitoring), MRTG (Traffic monitoring), Top (Traffic monitoring) and Kismet (Wireless scanning) which is available in the market. These tools generally used to monitor the network status but the hackers can use to hack the data. The information like bank account details, username, password, personal details and more will be hacked by the hackers and they can misuse the same.

This problem can be solved normally by using encryption and decryption algorithms (Cryptography). Encryption is a process of converting readable secret information into unreadable form (Cipher Text). Decryption is a process of converting the unreadable cipher text into readable form (plain text). Both sender of the data and the receiver of the data uses same key for encrypting and decrypting. But still the encryption and decryption algorithms have not given 100% security. The reason is that the hackers easily will find the key by capturing the packets and analyzing the chipper text using various software and hardware. In case of client-server architecture network, the servers authenticate the clients by login process. During the login process the client has to send the username and password. This username and password can be easily bypassed by the attacks like “SQL Injection”, where the validation is not done properly. Also using the virus and worm programs the hackers will collect the secret information from any node. Even the IP packet tracing to find the hacker or virus program developers, is a very tough job today. Since the virus programs will sit in another computer and do the needful. Much research has been conducted in the past to overcome the security issues in computer networks. Many encryption algorithms have developed and much security mechanisms got proposed, but till today we are facing many problems related to security.

To improve the security one can use another method to hide information and to send it through network without fear called stenography. It is an art of hiding information in multimedia elements like image, video and animation …etc. Generally, all the multimedia elements are stored in the storages devices as binary values. The binary values can be altered to hide secret information. Altering few bits may not change originality of the image, but if the changes are too high then, originality of the image will be spoiled. So to hide few kilo byte of information we need few megabytes of multimedia elements. Combining both stenography and cryptography together will improve the security dramatically.

In [12-5], G. Di Blasi and G. Gallo and M. Petrilia, has been produced composite images called Puzzle Image Mosaic (PIM). This method is inspired by Jigsaw Image Mosaic (JIM), where image tiles of arbitrary shape are used to compose the final picture. The JIM approach leads to impressive results, but the required computation time is high. An algorithm is proposed that produces good results in lower time. The technique takes advantage from recent results about data structures aimed to optimize proximity queries.

Experimental results prove the soundness of our method. Puzzle Image Mosaic (PIM). PIM is based on some recent techniques presented in Computer Graphics: Fast Photomosaic and Artificial Mosaic. Differently from JIM,

PIM does not perform any deformation of the tiles in order to create images more visually similar to Arcimboldi's paintings. Like Fast Photomosaic, PIM uses tiles containing small images and adopts the Antipole strategy to speed up the search process. Further, PIM makes use of the same algorithm proposed in Artificial Mosaic for directional guideline detection.

This proposed algorithm synthesizes mosaics with an acceptable cost, even on complex source images. "Photomosaic" transform an input image into a rectangular grid of thumbnail images. In this approach the algorithm searches in a large database of images for one that approximates. The resulting effect is very impressive. Recently Di Blasi and Petralia presented an approach to speed up the search process. I compare our performance with JIM in order to assess the quality of our method. It should be remarked that the comparison is not completely fair because the two algorithms are aimed to slightly different purposes.

JIM optimizes the final effect PIM tries to find a acceptable trade-off between performance and quality. Timing results show that, this algorithm is fast enough to be used as a plug-in in a typical user-end software. This operation is executed only once on the whole database. From an aesthetic point of view JIM is better than our algorithm, even if the results obtained by our method are very good. When we try to apply PIM to a very complex image (in terms of color variation and edge structure) it is not able to perform well; the output is comprised mainly by the imprecise directional guideline detection.

In [13-4], a new kind of mosaic has proposed by J. Kim and F. Pellacini namely Jigsaw Image Mosaic (JIM), where image tiles of arbitrary shape is used to compose the final picture. The generation of a Jigsaw Image Mosaic is a solution to the following problem, fill the container as compactly as possible with tiles of similar color to the container taken from the input set while optionally deforming them slightly to achieve a more visually pleasing effect.

We approach the problem by defining a mosaic as the tile configuration that minimizes a mosaicking energy function. We introduce a general energy-based framework for mosaicking problems that extends some of the existing algorithms such as Photo mosaics and Simulated Decorative Mosaics. We also present a fast algorithm to solve the mosaicking problem at an acceptable computational cost. We demonstrate the use of our method by applying it to a wide range of container images and tiles.

This proposed algorithm synthesizes mosaics with an acceptable cost, even on complex source images. In this approach, the algorithm searches in a large database of images for one that approximates. The resulting effect is very impressive. Recently Di Blasi and Petralia presented an approach to speed up the search process. I compare our performance with JIM in order to assess the quality of our method. It should be remarked that the comparison is not completely fair because the two algorithms are aimed for slightly different purposes.

JIM optimizes the final effect PIM tries to find an acceptable trade-off between performance and quality. Timing results show that this algorithm is fast enough to be used as a plug-in in a typical user-end software. This operation is executed only once on the whole database. From an aesthetic point of view, JIM is better than our algorithm, even if the results obtained by our method are very good. When we try to apply PIM to a very complex image (in terms of colour variation and edge structure) it is not able to perform well; the output is comprised mainly by the imprecise directional guideline detection.

In [13-4], a new kind of mosaic has proposed by J. Kim and F. Pellacini namely Jigsaw Image Mosaic (JIM), where image tiles of arbitrary shape are used to compose the final picture. The generation of a Jigsaw Image Mosaic is a solution to the following problem, fill the container as compactly as possible with tiles of similar colour to the container taken from the input set while optionally deforming them slightly to achieve a more visually pleasing effect.

As in Simulated Decorative Mosaics, the Jigsaw Image Mosaics maintain important edges found in the container image. While the first algorithm does so by reorienting the tiles, our approach uses oriented tiles of the best-fitting shape our framework has three major advantages. First, a user can easily control the result image by changing the weights in the energy formulation. Second, we can introduce new mosaicking generation rules by introducing additional energy terms in the energy formulation. Finally, the mosaic generation and tile preparation is completely automatic requiring no user intervention. Since the Jigsaw Image Mosaic problem can be cast as an instance of an energy minimization problem, various algorithms such as simulated annealing could be employed to find a solution.

Unfortunately, due to its high dimensional search space, most of the standard minimization techniques would demand too many resources to be run. This method also presents a fast minimization algorithm tailored to solve the generalized mosaicking problem. To efficiently compute a Jigsaw Image Mosaic, we propose an effective algorithm organized in three phases. In the first phase, we choose and roughly place the tiles, ignoring deformation. In the second phase, we refine the placement of each tile and deform them if necessary. Finally in the third phase, we assemble the final mosaic by placing each tile in its position and warping each image to its final deformed shape using the image warping technique. This method produces good results, and

is general enough to be applied to other ‘soft’ packing problems such as texture synthesis and product manufacturing.

In [14-3], Y. Dobashi, T. Haga, H. Johan, and T. Nisha proposed a non-photorealistic rendering method that creates an artistic effect called mosaicking. This method converts images provided by the user into the mosaic images. Commercial image editing applications also provide a similar function. However, these applications often trade results for low-cost computing. It is desirable to create high quality images even if the computational cost is increased. We present an automatic method for mosaicking images by using Voronoi diagrams.

The Voronoi diagrams are optimized so that the original image and the resulting image is as small as possible. Next, the mosaic image is generated by using the sites and edges of the Voronoi diagram. Graphics hardware can be used to efficiently generate Voronoi diagrams. A "Voronoi image" is an image being generatedby using Voronoi regions. A "reference image" is the image to be converted into the mosaic image. The method for creating mosaic images with a higher quality than currently available methods offer. In our method, the shapes of small regions in the mosaic image are approximated by using Voronoi diagrams.

To create the Voronoi diagrams, we make use of graphics hardware. This hardware can be utilized for fast generation of the Voronoi diagrams. This results in decreased computation time for the image generation processes. This method consists of two processes. In the first process, the mosaic image is automatically generated by creating the optimal Voronoi diagram so that the error between the original image and the resulting image becomes as small as possible. The second process allows the user to add various effects to the mosaic image created by the first step.

Thesecond process is designed in accordance with our observation of stained glass windows since stained glass is one of the applications that use mosaic images. One important feature is that there are color variations in each region of the stained glass. In previous methods, however, each tile in the mosaic image has a single color. The second process of our methodprovides ways to add these two visual effects, that is, edge enhancement and color variations in each tile. By using Voronoi diagrams, our method can generate the image that capture the features of the input image.

In [15-7], a novel approach for artificial mosaic generation is proposed by. The high frequency details are managed in a global way allowing to preserve the mosaic-style also for small ones. Here, we adopt a "one-after-one" tile positioningand orienting strategy.The proposed approach uses Gradient Vector Flow (GVF). GVF is able to capture the overall gradient behaviorin a proper way.

The main novelty introduced in thispaper is a new way to deal with high-frequency details. Almostall previous approaches filtered-out such componentsto simplify the tile positioning heuristics. We use GVF of a raster image to guide the positioning of the tiles.GVF computation simplifies tile positioning, because thegeneration process of the flow is constrained to be smooth,maintaining at the same time the information of the small details.GVF is a field of vectors that minimizes the followingenergy function. The GVF force field can be used to effectively drive tiles positioning. Edge information is preserved; it is propagated in the close regions and merged together in a smooth way. A first advantage of the novel technique is that it is able to better preserve fine details. This happens because high frequency areas are proprietarily filled. This technique overcomes explicit edge detection using the Gradient Vector Flow. This technique does not cut tiles.

Art often provides valuable hints for technological innovations especially in the field of Image Processing and Computer Graphics. Here, we survey in a unified framework several methods to transform raster input images into good quality mosaics. For each of the major different approaches in literature the paper reports a short description and a discussion of the most relevant issues. To complete the survey comparisons among the different techniques both in terms of visual quality and computational complexity are provided.

The main purpose and its aim may be to reproduce the aesthetic essence of arts by mean of computational tools.The focus of this method is to review the state of the art for the problem of digital mosaic creation. The survey restricts its scope only to the techniques that explicitly bear the “mosaic” name and that make use of primitives largerthan pixels, points or lines. Stippling and hatching are hence not covered here, although their visual similarityto mosaic naturally leads to approaches for thesetechniques that closely resemble the mosaic techniques.

The creation of a digitalmosaic resembling the visual style of an ancient lookingman-made mosaic is a challenging problem because it hasto take into account the polygonal shape of the tiles, thesmall size of the tiles, the need to pack the tiles as denselyas possible and, not last, the strong visual influence that tile orientation has on the overall perception of the mosaic. In particular orientation cannot be arbitrary but it is constrained to follow the gestalt choices made by the author of the source picture. Tiles, hence, must follow andemphasize the main orientations chosen by the artist.

From the survey it is identified that no steganography is perfect in all situations. In the literature lot of algorithms are there to hide the information in an image

file but most of it consumes high resource for completing the task which is not suitable for light weight mobile devices [1], [2]. Few basic algorithms like 1LSB, 2LSB and 3LSB methods in the literature are suitable for mobile devices since the computational complexity is very low. But, these methods either lack in maintaining the originality of the source image or in increasing the number of bits to be embedded. Furthermore, every algorithm in the literature has it's own merits and demerits and we cannot predict which algorithm is best or worst since, based on the parameters such as size of the cover image, content of the cover image, size of the plain text, content of the plain text, and encryption algorithm used to generate the cipher text the steganography schemes may produce best or worst result with respect to computational complexity, capacity, and detectable distortion.

Hence a new work has to be developed that takes cover image and plain text as the input and returns the steganoimage. The steganoimage has to be generated by analyzing various parameters and by applying the right steganography scheme.

3. Proposed Work

In our proposed method, the color value of each pixel is grouped in to three categories; dark, bright and medium. The dark pixel values can be incremented, the bright pixel values can be decremented and the medium pixel value can be either incremented or decremented. By following this idea, the change in the pixel value may not be identified easily by the users. Based on the encrypted (proposed encryption technique mentioned below) cipher text (Numerical values) each pair (odd and even) of pixels has to be examined. The cipher text is in the form of numbers between 0 to 40. These differences have to be recorded in the pixel pair either by incrementing or decrementing any one or both the pixel. If the change is too high then the pixel pair has to be ignored without embedding the data. If the change in the pixel value is below an accepted range then the data has to be embedded.

By doing this, large amount of data's can be embedded just by altering few LSBs to achieve good capacity. In this proposed method the hacker may not know, how much LSB has to read from each pixel [12]. Also hacker may not know about which pair contain data and which pair contain no data. So, the security will also improve without increasing detectable distortion (DD). As all the three factors which affect the performance of stenography improved by our proposed system, the Steganalysis is very hard.

Enhancing Security via Encryption

Even though the above said method improves capacity, security and reduces DD, it is not sufficient for the current need. Providing security is a challenging work in the today's network. So, it is better to propose a new encryption algorithm which is suitable for our above said bit embedding scheme.

In out proposed encrypting algorithm, the frequency of the alphabet in the dictionary is considered. The alphabet with highest frequency can be replaced with number one. The next highest frequency alphabet can be replaced with number two. Similarly, the alphabet with lease frequency in the dictionary will be replaced with 26. For the character '1', '2', '3' and so on, the number 27,28,29 and so. For some frequently used special characters like space, hyphen (-), exclamatory (!) symboletc the last range of values can be substituted.

This technique is suitable for our proposed bit embedding scheme, since, the maximum difference between the pixels value could be just 40. Also the maximum difference will occur rarely according to the alphabet frequency in the dictionary [15]. Hence this transposition technique is good for the proposed bit embedding scheme.

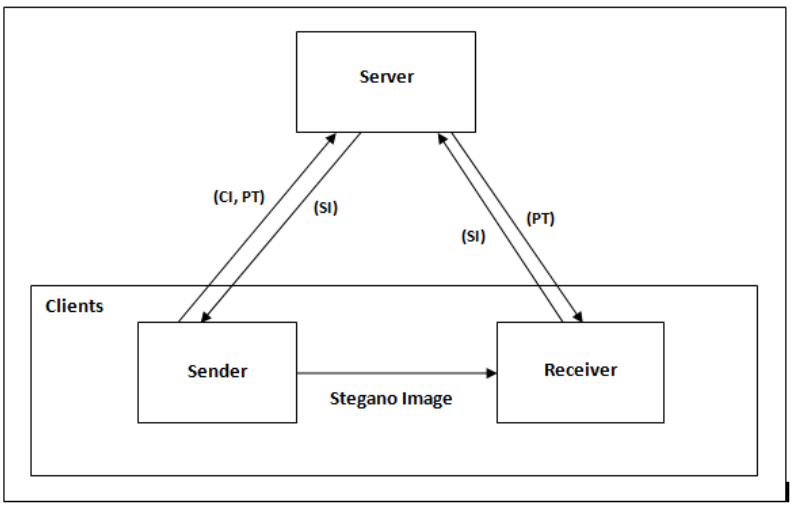

Fig. 4.1 System Architecture

3.1 Advantages of Proposed System

- Low visible distortion.
- High capacity.
- Less Computational Complexity.

The system proposed by this work takes the previous existing problem into account and it combines the art of steganography with cryptology. It encodes a message and then, hides it in a file. This makes the message unreadable even after it is disclosed. By this way we can conceal our information. This work hides text files inside JPEG files and creates a JPEG file with secret message. A key should be given by the user to encode the message. The message is first encoded with this key and then embedded inside the specified file.It is then stored as per the name specified.To reveal the message that is inside a file, one should give the right key and then this key will decrypt the message and then the embedded message is extracted out for viewing. If an attempt is made with a wrong key, a warning is made to tell that that key is invalid. By this method we hide our secret message from invalid users. Several options are provided for the users so that they work in a modish environment. Users are provided with a facility to locate the files on the system through browsing.

4. Implementation Details

This work contains three modules namely “Server”, “Sender”, and “Receiver”. The “Server” module contains 8 sub modules such as 1LSB, 2LSB, 3LSB, 4LSB, RGB1, GB1, RGB2, and GB2. All these modules can been implemented fully in phase II and two modules have been implement in this phase I. Both the modules have been deployed and tested for bug’s free operation.

4.1 Server

This module takes cover image and plain text as the input from the sender clients and returns the steganoimage to the sender clients. The steganoimage will be generated by analyzing the above said parameters and by applying the right steganography scheme. The proposed work helps in reducing the detectable distortion, computational complexity of the client device, and in increasing the capacity. This module receives cover image and secret information from the sender client and it will analyze both the image and information and based on the parameters such as number of pixels, number of bits in the secret information, content of the image, and content of the secret information. Based the analysis result any one of the steganography schemes such as 1LSB, 2LSB, 3LSB, 4LSB, RGB1, GB1, RGB2, and GB2 will be applied.

Further this module takes stegano image as the input from the receiver clients and returns the secret information to the receiver clients. The secret information will be generated by processing the stegano image and by identifying the bit embedding scheme applied already.

4.2 Sender

This module provides a GUI to the users for entering the secret information and for locating the cover image. Through this GUI the users can enter the text to be send securely to the receiver and he/she can select a cover image from the local or remote storage. After getting these information from the user it will forward the same to the web server for getting the stegano image. The received stegano image will contain the embedded secret information which cannot be identified by others. The sender need not to spent much resource such as CPU, and Memory for getting the stegano image since all the computational tasks have been done by the server. Further the sender can send the stegano image to the receiver.

4.3 Receiver

This module receives the stegano image form the sender that contains the embedded secret information which cannot be identified by the receiver or others easily. The receiver will forward the same to the server for extracting the secret information. The receiver need not to spent much resource such as CPU, and Memory for getting the secret information since all the computational tasks have been done by the server. Further this module provides a GUI to the users for viewing the secret information. Through this GUI the users can read the text sent by the sender.

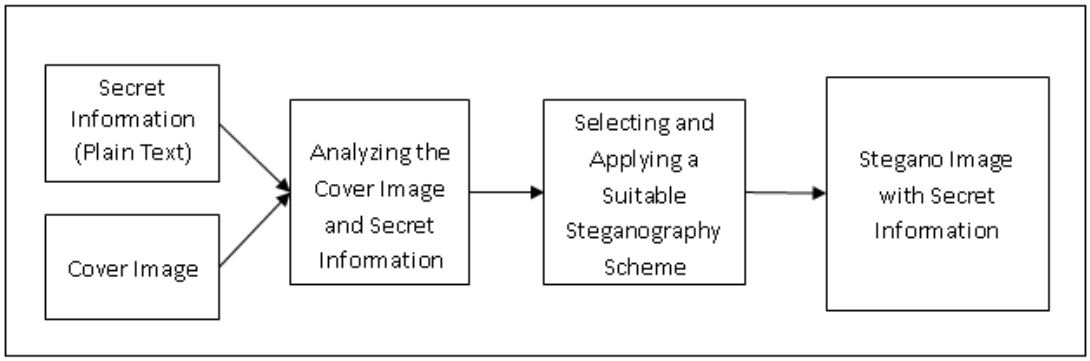

Fig. 4.2 Server Side Process

5. RESULT AND DISCUSSION:

The proposed work reduces the detectable distortion, computational complexity of the client device, and it increases the capacity significantly. The experimental result says that, the proposed system performs better than the legacy schemes such as 1LSB, 2LSB, 4LSB, and few other legacy schemes with respect to the capacity, computational complexity, and detectable distortion. It maintains the detectable distortion of an image equal to the 1LSB method and it offers capacity equal to the 4LSB method. Thus it offers four times higher capacity and four times lesser detectable distortion. Also, majority of the computation is happening at server side and thus it consumes lesser computational power of the devices. Thus it is suitable for low end mobile devices.

6. CONCLUSION

Hiding a message with steganography methods reduces the chance of a message being detected. However, if that message is also encrypted, if discovered, it must also be cracked (yet another layer of protection). Steganography combined with cryptography becomes a powerful tool for security. In the near future, the most important use of stenographic techniques will probably be lying in the field of digital watermarking. Content providers are eager to protect their copyrighted works against illegal distribution and digital watermarks provide a way of tracking the owners of these materials. Although it will not prevent the distribution itself, it will enable the content provider to start legal actions against the violators of the copyrights, as they can now be tracked down.

In this work we have discussed in detail about the steganography, security issues in computer networks and MPEG encryption. We have proposed a new scheme of bit embedding which has many advantages. It improves the security and reduces the DD. In this work we have discussed in detail about the steganography, security issues in computer networks and MPEG encryption. We have proposed a new scheme of bit embedding which has many advantages. It improves the security and reduces the DD. But still it has to improve further in the future to reduce the computational complexity and the current version is not suitable for mobile devices with very low connectivity and computing speed.

REFERENCE:

[1]. V Saravanan, V Mohan Raj, Maximizing QoS by cooperative vertical and horizontal handoff for tightly coupled WiMAX/WLAN overlay networks, Journal of Networks, Software Tools and Applications, vol. 19, no. 3, pp. 1619-1633, 2016.

[2]. V Saravanan, A Sumathi, Dynamic handoff decision based on current traffic level and neighbor information in wireless data networks, Fourth International Conference on Advanced Computing (ICoAC), pp. 1-5, 2012.

[3]. V Saravanan, S Thirukumaran, M Anitha, S Shanthana, Enabling self auditing for mobile clients in cloud computing, International Journal of Advanced Computer Technology, vol. 2, no. 3, pp. 53-60, 2013.

[4]. V Saravanan, A Sumathi, Handoff mobiles with low latency in heterogeneous networks for seamless mobility: A survey and future directions, European Journal of Scientific Research, vol. 81, no. 3, pp. 417-424, 2012.

[5]. Kaur and S. Behal, "A Survey on various types of Steganography and Analysis of Hiding Techniques," International Journal of Engineering Trends and Technology, vol. 11, no. 8, pp. 388-392, 2014.

[6]. H. Zhang and H. Tang, "A Novel image steganography algorithm against statistical analysis," proceeding of the IEEE, vol. 19, no. 22, pp. 3884-3888, Aug. 2007.

[7]. J. Fridrich, M. Goljan, and R. Du, "Detecting LSB Steganography in Color and Gray-Scale Images," Magazine of IEEE Multimedia Special Issue on Security, pp. 22-28, Nov. 2001.

[8]. V Saravanan, V Mohan Raj, A Seamless Mobile Learning and Tension Free Lifestyle by QoS Oriented Mobile Handoff, Asian Journal of Research in Social Sciences and Humanities, vol. 6, no. 7, pp. 374-389, 2016.

[9]. A Sumathi, V Saravanan, Bandwidth based vertical handoff for tightly coupled wimax/wlan overlay networks, Journal of Scientific & Industrial Research, vol. 74, pp. 560-566,2015.

[10]. S.A. Halim and M.F.A Sani. "Embedding using spread spectrum image steganography with GF ( )," in Proc. IMT-GT-ICMSA, 2010, pp. 659-666.

[11]. P. Kruus, C. Scace, M. Heyman, and M. Mundy. (2003), "A survey of steganography

a. Techniques for image files." Advanced Security Research Journal.

[12]. B. Li, J. He, J. Huang, and Y.Q. Shi. (2011, Apr.). "A survey on image steganography and Steganalysis." Journal of Information Hiding and Multimedia Signal Processing. 2(2), [Online], pp. 142-172

[13]. Niels Provos and Peter Honeyman, Hide and seek: An introduction to steganography, IEEE Security and Privacy, vol. 1, no.3, pp. 32-44, 2003.

[14]. Fridrich, J., Goljan, M., Soukal, D.: Perturbed quantization steganography. ACM Multimedia System Journal 11(2), 98–107 (2005)

[15]. Tomas Pevny and Jessica Fridrich, "Benchmarking for steganography", Proc. of the 10th International Workshop on "Information Hiding", vol. 5284, pp. 251-267, 2008.

[16]. Marin, G.A., "Network security basics," Security & Privacy, IEEE, vol.3, no.6, pp. 68-72, Nov.-Dec. 2005

[17]. J. Fridrich, D. Soukal, and M. Goljan, "Maximum likelihood estimation of secret message length embedded using pmk steganography in spatial domain", Proc. of IST/SPIE Electronic Imaging: Security, Steganography, and Watermarking of Multimedia Contents VII, vol. 5681, pp. 595-606, 2005.

[18]. Kartalopoulos, S. V., "Differentiating Data Security and Network Security," Communications, 2008. ICC '08. IEEE International Conference on, pp.1469-1473, 19-23 May 2008.

[19]. Landwehr, C.E., Goldschlag, D.M., "Security issues in networks with Internet access," Proceedings of the IEEE, vol.85, no 12, pp.2034-2051, Dec 1997.

[20]. Haz Malik, K. P. Subbalakshmi, and Rajarathnam Chandramouli, Steganalysis of qim-based data hiding using kernel density estimation. Proc. of the 9th ACM Workshop on Multimedia and Security, ACM Press, pp. 149-160, 2007.

[21]. V Saravanan, V Mohan Raj, Maximizing QoS by cooperative vertical and horizontal handoff for tightly coupled WiMAX/WLAN overlay networks, Journal of Networks, Software Tools and Applications, vol. 19, no. 3, pp. 1619-1633, 2016.

[22]. V Saravanan, A Sumathi, Dynamic handoff decision based on current traffic level and neighbor information in wireless data networks, Fourth International Conference on Advanced Computing (ICoAC), pp. 1-5, 2012.

[23]. V Saravanan, S Thirukumaran, M Anitha, S Shanthana, Enabling self auditing for mobile clients in cloud computing, International Journal of Advanced Computer Technology, vol. 2, no. 3, pp. 53-60, 2013.

[24]. V Saravanan, A Sumathi, Handoff mobiles with low latency in heterogeneous networks for seamless mobility: A survey and future directions, European Journal of Scientific Research, vol. 81, no. 3, pp. 417-424, 2012.