Analyzing the Terrorist Social Networks with Visualization Tools

Christopher C. Yang[1], Nan Liu[1], and Marc Sageman[2]

[1] Department of Systems Engineering and Engineering Management
The Chinese University of Hong Kong
[2] The Solomon Asch Center for Study of Ethnopolitical Conflict
The University of Pennsylvania

Abstract. Analysis of terrorist social networks is essential for discovering knowledge about the structure of terrorist organizations. Such knowledge is important for developing effective combating strategies against terrorism. Visualization of a network using a 2D graph can greatly facilitate the inspection of the global structure of the network with the support of the social network analysis techniques. However, its usefulness becomes limited when the size and complexity of the network increase. In this work, we study the use of two interactive visualization techniques in the visualization of complex terrorist social networks: fisheye views and fractal views. Both techniques facilitate the exploration of complex networks by allowing a user to select one or more focus points and dynamically adjusting the graph layout and abstraction level to enhance the view of regions of interest. Combining the two techniques can effectively help an investigator to recognize patterns previously unreadable in the normal display due to the network complexity. Case studies are presented to illustrate how such visualization tools are capable to extract the hidden relationships among terrorists in the network through user interactions. Experiment was conducted to evaluate the performance of the visualization techniques.

Keywords: Terrorist social networks, social network analysis, information visualization, fisheye views, fractal views

1.Introduction

As a type of organized crime, terrorism requires the collaboration among a number of terrorists. The relationships among different terrorists form the basis of a terrorist organization and are essential for its operations [2], [14]. An effective model for capturing the structure of a terrorist organization is the network model in which individual terrorists and their relationships are represented by nodes and links respectively. Terrorist social networks fall into the large category of social networks. While social networks have been successfully used to model the structure of communication networks and the World Wide Web, it is also especially appropriate for investigations in terrorism [1]. An investigator of a terrorist social network typically performs the following tasks [4]:

Subgroup Detection: Different members of a terrorist social network may form groups that perform different functions of the entire organization [6]. For instance, there may exists different responsible for handling recruitment, money laundering, training, etc. They may also form teams or cell groups that carry out different operations, such as the Hamburg cell responsible for the 9/11 attack and the Montreal cell which attempted the Millennial Plot. Detecting such groups helps an investigator to swiftly identify the related offenders given only a few known suspects.

Identification of Important Actors and their Roles: Different individuals usually play different roles in their groups. For example, some key member may act as a leader that controls the activities of the whole group. Some may serve as gatekeepers to ensure the communication and coordination between different groups of a larger network. Removal of these important actors is critical for untangling and disrupting a terrorist social network.

Discovery of Patterns of Interaction: Patterns about how different individuals and groups are associated can help reveal the overall structure of a criminal network, which often reveals the points of vulnerability [3],[6]. A very common task an investigator performs is to find significant paths of associations between different individuals that may generate investigative leads and uncover hidden information.

Traditional terrorist social network analysis and social network analysis in general is mainly a manual process. An investigator has to spend a large amount of time performing data base searches and reading reports in an attempt to identify useful entities and relationships in a large network. This is both time-consuming and labor-intensive. To facilitate social network analysis, modern systems such as COPLINK [5] employs visualizations such as a 2D graph to present a network. In a 2D graphical portrayal of a social network, the stronger the association between two nodes or two groups, the closer they appear on the graph; the weaker the association, the farther apart. Xu and Chen [7] has adopted the metric multidimensional scaling algorithm to visualize the criminal social networks. While a static graphical layout suffices to reveal the structure of relatively small and simple networks, it is usually not effective enough for the manual exploration of large and complex networks. In this work, we propose to use interactive visualization techniques such as fisheye views and fractal views for facilitating the analysis of complex social networks and demonstrate its use in the analysis of a large terrorist network, the global Salafi Jihad (the violent, revivalist social movement of which al Qaeda is a part) [14].

2.Terrorist Social Network – Global Salafi Jihad

A social network is typically represented by a weighted graph $G = (V, E; w)$, where V corresponds to the set of nodes, E is the set of links, w is a function mapping each link $(u,v) \in E$ to a weight w_{uv} in the range [0,1] that indicates the strength of association between u and v. Each node, v, is corresponding to a person, which is a terrorist in a terrorist social network (TSN). A link between two nodes (terrorists), *(u,v)*, represents that there are some kinds of relationships between the corresponding terrorists, *u* and *v*. The weight w_{uv} is determined by the number of types of relationships existing between *u* and *v*. Two terrorists can be related through different types of associations. We have heuristically assigned an importance score s_r to each type of relationship *r* and compute a total score s_{uv} for each link (*u*, *v*) as the total score of the relationships between *u* and *v*, i.e.,

$$s_{uv} = \sum_{r \in R(u,v)} s_r$$

where *R(u,v)* denotes the set of relationships existing between *u* and *v*. The link weight w_{uv} is then computed as the normalized link score, i.e.,

$$w_{uv} = \frac{s_{uv}}{\max_{u,v \in V}(s_{uv})}$$

In this work, we have adopted the data available from an authoritative terrorism monograph, authored by Sageman [14], to build the terrorist social network of the global Salafi Jihad. Sageman is a forensic psychiatrist an expert on Al-Qaeda. He is a former CIA case officer, who has worked closely with Afghanistan's mujahedin. He has advised various branches of the U.S. government in the war of terror. In the global Salafi Jihad social network, there are totally 366 terrorists described in the data set, which is given as a list of records with the same schema, one record for each terrorist. Each record includes two types of information: terrorist's properties such as name, alias, date of birth, etc. and his relationships with other terrorists, which include 6 types: acquaintance (r_1), friends (r_2), relatives (r_3), nuclear family member (r_4), teachers (r_5), and religious leader (r_6). Based on the data set, the resulted terrorist social network consists of a total of 366 nodes and 1275 links.

3.Visualization of Terrorist Social Networks

The computation of initial node coordinates and sizes are the most important steps in presenting the terrorists and their relationships, represented as a weighted graph *G* = (*V, E; w*), on a two-dimensional space. A mapping of each node $v \in V$ of the terrorist social network to a point $p_v = (x_v, y_v) \in \mathbb{R}^2$, the coordinates of *v* on the plot, is needed.

There are several desirable properties of an effective visualization: (1) Nodes should be separated by an optimal distance in order to fully utilize the two-dimensional space instead of being cluttered (2) The length of a link should reflect the strength of association between the two end nodes, i.e., two connected nodes should appear closer if they are strongly associated, and distant if the association is weak. (3) The crossing of edges should be minimized so the user can clearly see the relationships between nodes. (4) The size of a node should be proportion to the importance of the corresponding terrorist.

3.1 Computing Node Coordinates

We utilize the spring embedder algorithm [8] to initialize the coordinates of the nodes in the terrorist social network to achieve objectives (1) to (3) as described above. The spring embedder algorithm models nodes as charged particles with mutual repulsion and links as springs attached to their end nodes. It produces a 2D layout of the network by finding a (locally) minimum energy state of this physical system. The repulsive force is introduced to avoid having the nodes cluttered together while the spring force tries to maintain a desirable distance between nodes.

Spring Embedder Algorithm:

1. Specify natural length of spring l_{uv} for each $(u,v) \in E$ which controls the desirable distance between u and v

   $l_{uv} = l_{max}$ (1-w_{uv}) where l_{max} is an upper limit on the length of links
2. Randomly initialize the node position p_v of node v for all $v \in V$
3. Compute the force acting on nodes $F(v)$

   $$F(v) = \sum_{u \in V \setminus \{v\}} F_{repulsion}(u,v) + \sum_{u \in N(v)} F_{spring}(u,v)$$

   where $N(v)$ denotes the set of nodes linked to v in the network.

   $$F_{repulsion}(u,v) = \frac{R}{\|p_u - p_v\|^2} \cdot \overrightarrow{p_u p_v}$$

   where R is a repulsion constant

   $$F_{spring}(u,v) = S \cdot (\|p_u - p_v\| - l_{uv}) \cdot \overrightarrow{p_u p_v}$$

   where S is the stiffness parameter of the spring
4. Update node positions p_v

   $p_v = p_v + \mu \cdot F(v)$

   where the step length μ is usually a very small number
5. Repeat Step 3 and 4 until $F(v) = 0$

3.2Computing Node Size

Each node v is displayed as a circle, whose size is controlled by its radius r_v. For the purpose of terrorist social network analysis, a node's prominence is largely determined by its centrality [4]. In particular, we employed two centrality measures: degree and closeness. A node's degree $c_{degree}(v)$ is the number of links attached to it. An individual having a high degree may imply leadership while an individual with high closeness is more likely to serve as a mediator in the network. A node's closeness $c_{closeness}(v)$ is the inverse of the sum of its distances to all other nodes in the network,

i.e., $$c_{closeness}(v) = \frac{1}{\sum_{v \neq u \in V} \| p_u - p_v \|}.$$

In our system, a user may choose either measure to determine the nodes' sizes.

(a) **(b)**

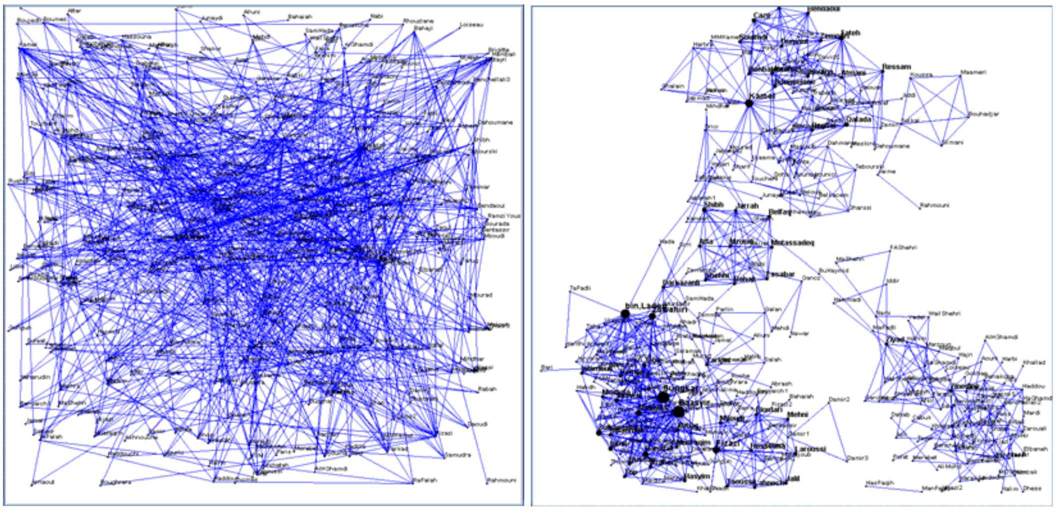


Figure 1: (a) Initial Layout (b) Layout after applying the spring embedder algorithm,

In Figure 1 (a), the Global Salafi Jihad social network without using the spring embedder algorithm for initialization is presented. The nodes are spread out to optimize the usage of the rectangular space. However, the natural clusters of the terrorist groups cannot be found and the distance between any two terrorists does not correspond to their strength of associations. After utilizing the spring embedded algorithm, four natural clusters can be identified as shown in Figure 1 (b). These clusters correspond to the central staff of as Qaeda, Core Arabs, Maghreb Arabs, and Southeast Asians. Using the measurement of degree and closeness of the nodes to compute their sizes, as illustrated in Figure 1 (b), the important persons or leaders of each cluster can be extracted visually.

4.Focus-plus-Context based Visualization of Social Networks

The number of links within a network usually grows at a much faster rate than the number of nodes. As a result, the produced layout would unavoidably contain clusters of densely connected nodes. Many of the local details become unreadable due to the crossing of edges and the high density of nodes such as the lower left region in Figure 1 (c). In information visualization, this problem is known as visual load [9]. A commonly used simple technique is to provide a zoom-in function, which could linearly magnify the drawing so that less information is presented in the zoom-in window. However, the global structure cannot be retained and manual integration is required to incorporate the zoom-in window with the global structure. Alternatively, a higher dimensional space such as 3D space can reduce the visual load by increasing the volume of space. However, a 3D layout has to entail more complicated operations, which is unfavorable for unsophisticated users. Moreover, it would also be harder to observe the global structure of the network in a 3D space.

Investigators solving a particular crime usually have some prior knowledge regarding certain members of the social network under study. For instance, for a homicide case, the victim and his acquaintance may be known and sometimes an investigator may have initial guesses about possible suspects. The major utility of visualization is helping the investigator uncover unknown knowledge embedded in the complex network based on the limited known information. A typical process employed by an investigator is to start from some known entities, analyze the associations they have with other entities, if some interesting association is uncovered, one may follow such a lead and keep expanding the associations until some significant link is uncovered between seemingly unrelated entities. During such a process, at different moments, a user is more concerned about information associated with particular nodes, which we refer to as focuses, than that about the network as a whole. However, a static layout as produced by methods like spring embedder provides no support of this kind of focus dependent analysis. In this section, we propose to use focus-plus-context information visualization techniques, which aim at assisting a user to explore particular parts of a complex network.

The focus-plus-context visualization [17] is a type of interactive visualization. It allows a user to select one or more *focuses*, which would be nodes in the case of social networks, and dynamically adjust the layout of the network based on the focuses in order to enhance the view of the focuses and their surrounding context. Fisheye views and fractal views are two particular kinds of focus-plus-context visualization techniques [18], [19]. Both techniques have been applied to visualize the self-organize maps for Internet browsing. Fisheye view is a kind of nonlinear magnification technique. It maintains the same screen size by magnifying the region surrounding the focus while compressing the distant regions without losing the global structure of the network. Fractal view identifies a focus's context based on its associations with other nodes. It enhances the view of focus and its context by reducing less relevant information. Fisheye views and fractal views could complement each other. Combining the two techniques could produce very effective focus-plus-context view of complex networks. It is proven that fisheye views and fractal view are successful to support users in exploring the details of the self organizing maps which are impossible before such techniques are applied. However, they have not been applied to visualize a network structure such as terrorist social networks. It has not been investigated how fisheye views and fractal views can perform in analyzing the relationships among the nodes in a high density social network. Besides, the fractal views for self-organizing maps are developed based on the adjacency of the two-dimensional regions while the fractal views for terrorist social networks are developed based on the links and shortest paths of the networks.

4.1Fisheye View

Fisheye views, first proposed by Furnas [10] and further enhanced by Marchionini and Brown [11], are known as distortion techniques in information visualization. Regions of interest are enlarged and the other regions are diminished so that one or more parts of a view are emphasized. Both local details of the regions of interest and global structure of the overall display are maintained. By specifying the focus point(s), users may enhance the views of particular regions of the two dimensional display of the network.

(a) (b)

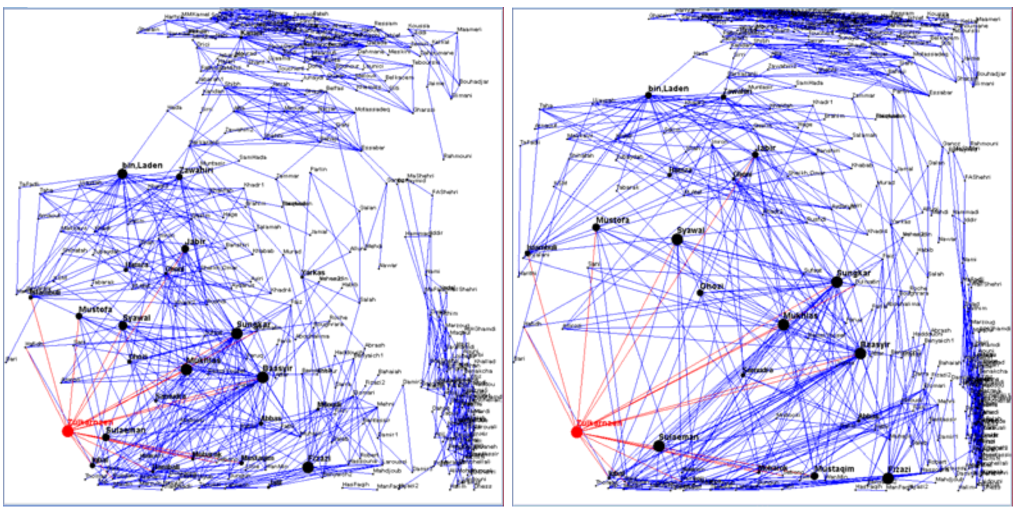


Figure 2: (a) Fisheve View with d = 2 (b) Fisheye View with d = 6

Using fisheye views, we transform a node' normal coordinates, (x_{norm}, y_{norm}) into the fisheye coordinates, (x_{feye}, y_{feye}) based on the focus point, (x_{focus}, y_{focus}) using Polar transformation. Equation (1) presents the Cartesian transformation.

$$< x_{feye}, y_{feye} > \; = \; < x_{focus} + r_{feye}\cos\theta, y_{focus} + r_{feye}\sin\theta > \qquad (1)$$

where

$$r_{feye} = r_{norm} \cdot \frac{d+1}{d \cdot \frac{r_{norm}}{r_{\max}} + 1}$$

$$r_{norm} = \sqrt{(x_{norm} - x_{focus})^2 + (y_{norm} - y_{focus})^2}$$

$$\theta = \tan^{-1}\left(\frac{y_{norm} - y_{focus}}{x_{norm} - x_{focus}}\right)$$

The constant d is the *distortion factor*. When d equals zero, there is not any magnification of the focus area. As d increases, the focus and its context will be magnified and the further regions will be diminished. r_{max} corresponds to the maximum possible value of r in the same direction as θ.

Figure 2 (a) and (b) illustrate the fisheye views using Cartesian transformation with distortion factor as 2 and 6, respectively. Figure 2 (c) and (d) present the fisheye views using polar transformation with distortion factor as 2 and 6, respectively.

4.2 Fractal View:

Fractal view belongs to another class of information visualization techniques known as information reduction. It controls the amount of information displayed by focusing on the syntactic structure of the information. Fractal view [12] utilizes the concept of Fractal [13] to abstract complex objects and controls the amount of information displayed with a threshold set by users. In order to apply the fractal views, we first generate a hierarchical structure capturing the syntactic relationships between the focus and other nodes. The network topology is transformed into a hierarchy by extracting a tree from the network that has the focus at its root and other nodes at the branches and the leaves. Each path from the focus to another node in this tree should establish the strongest association between the two nodes. As the length of each in the network corresponds to the strength of association between two connected nodes, the total length of a path is a good indicator of the strength of the association along the path. Therefore, we generate this tree structure by finding the shortest paths from the focus to every other node in the network using the famous single source shortest path algorithm [15]. The fractal values of the nodes in the tree are determined by propagation from the root to other nodes based on the following procedure:

1. Fractal value of the focus = F_{focus} = 1
2. Other nodes' fractal values are determined based on the fractal value of their parent node as follows:

$$F_c = \left(\frac{w_{cp}}{\sum_{c' \in children\_of(p)} w_{c'p}}\right)^{-1/D} F_p$$

where c is a child of p; w_{cp} denote the association weight between c and p; the constant D corresponds to the fractal dimension. The association weights are taken into account so that a parent node will propagate more fractal value down to the child nodes which are more strongly associated with the parent.

A higher fractal value indicates the node is more closely related to the focus. The degree of abstraction can be controlled by a threshold on the fractal value. Only nodes with a fractal value above the threshold will be kept visible while those with fractal values below the threshold are considered less relevant to the current focus and are not displayed. Figure 3 illustrates the effect of fractal view with different thresholds. The number of nodes filtered increases as the threshold increases. By hiding nodes with low fractal values, the complexity of the network could be effectively simplified, which enables a user to focus more on the relationships between the focus and those closely related nodes. Figure 3 (a) and (b) illustrate the fractal views of the network in Figure 2 (d) with factual value threshold as 0.3 and 0.7, respectively.

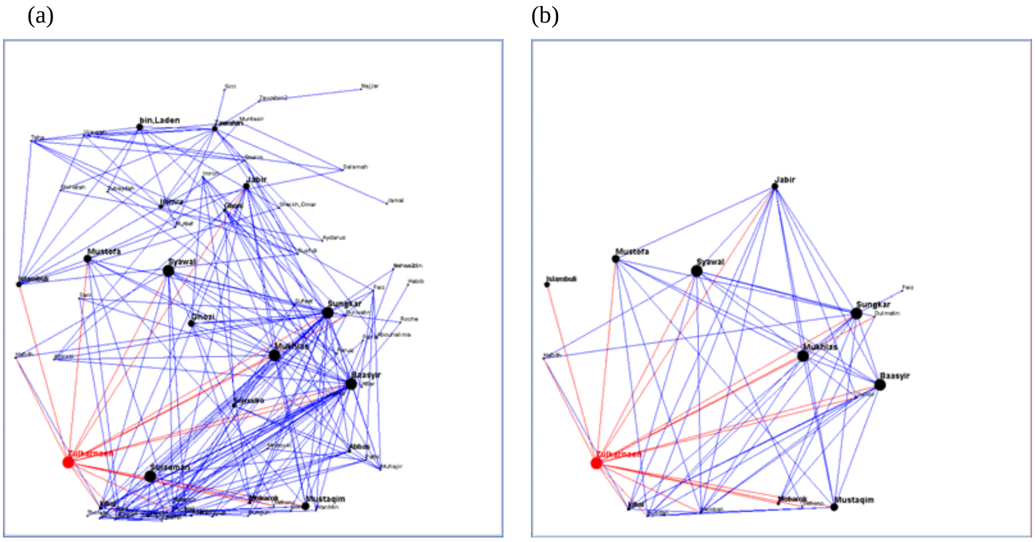


Figure 3: Fractal Views produced on the basis of Figure 2 (d)

(a) Fractal Value Threshold = 0.3

(b) Fractal Value Threshold = 0.7

4.3 Fisheye Views and Fractal Views with Multiple Focuses

Multiple focuses can be useful when a user wants to magnify several local regions or to uncover the associations between indirectly connected nodes. To determine a node's fisheye coordinates and radius under multiple focus points, we first compute a node's fisheye coordinate (x^i_{feye}, y^i_{feye}) and radius r^i_{feye} when focus i is effective. The set of (x^i_{feye}, y^i_{feye}) and r^i_{feye} are then averaged to obtain the node's final coordinate and radius

$$(x_{feye}, y_{feye}) = \sum_{i}^{K} (x^{i}_{feye}, y^{i}_{feye}) \Big/ K$$

$$r_{feye} = \sum_{i}^{K} r^{i}_{feye} \Big/ K$$

where K is the number of focuses selected by the user.

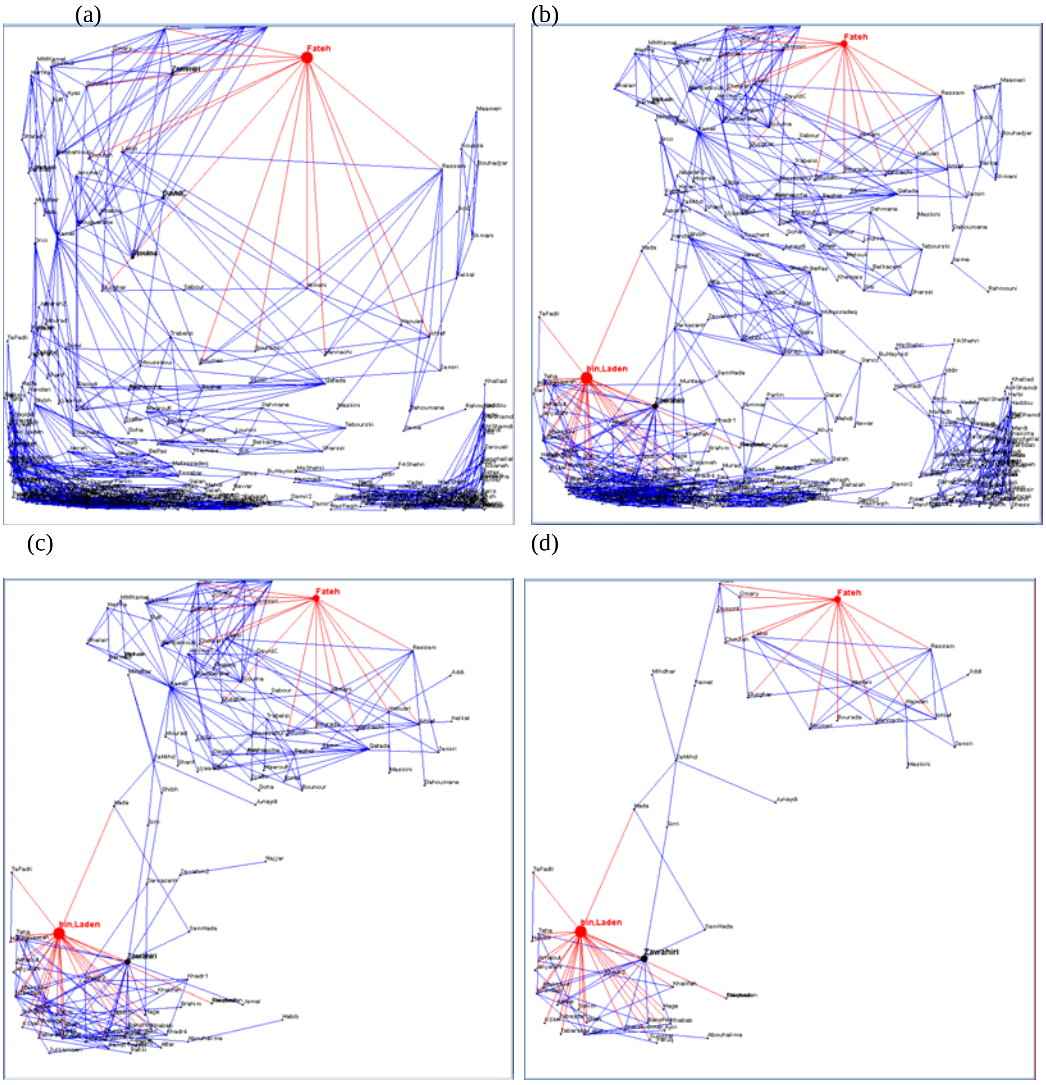


Figure 4: Fisheye and Fractal View with Multiple Focuses

(a) Fisheye view with single focus Fateh,
(b) Fisheye view with both Fateh and Bin Laden as focus
(c) Combined fisheye and fractal view with both Fateh and Bin Laden as focus and a fractal value threshold 0.3
(d) Combined fisheye and fractal view with both Fateh and Bin Laden as focus and a fractal value threshold 0.6

The fisheye view in Figure 4(a) is produced with only one focus Fateh, whose surrounding regions is magnified. Figure 4(b) is produced using the same fisheye distortion factor but with one more focus Bin Laden. As can be seen, the degree of magnification of the region around Fateh so that the regions around both Fateh and Bin Laden could both be magnified.

To determine a node's fractal value under multiple focuses, we generate a shortest path tree for each of the focuses. A node's fractal value is computed as the average of the fractal values propagated to it based on this set of trees. Accordingly, a node with a high fractal value under multiple focuses must be strongly connected with all or most of the selected focuses and could be considered as good intermediaries between the focuses. Figure 4(c) and Figure 4(d) illustrates the effect of fractal view with two focus points. As the fractal threshold is increased from 0.3 in Figure 4(c) to 0.6 in Figure 4(d), many nodes that are associated with only one of the focuses got removed while those between the two focuses got retained.

4.4 System User Interface:

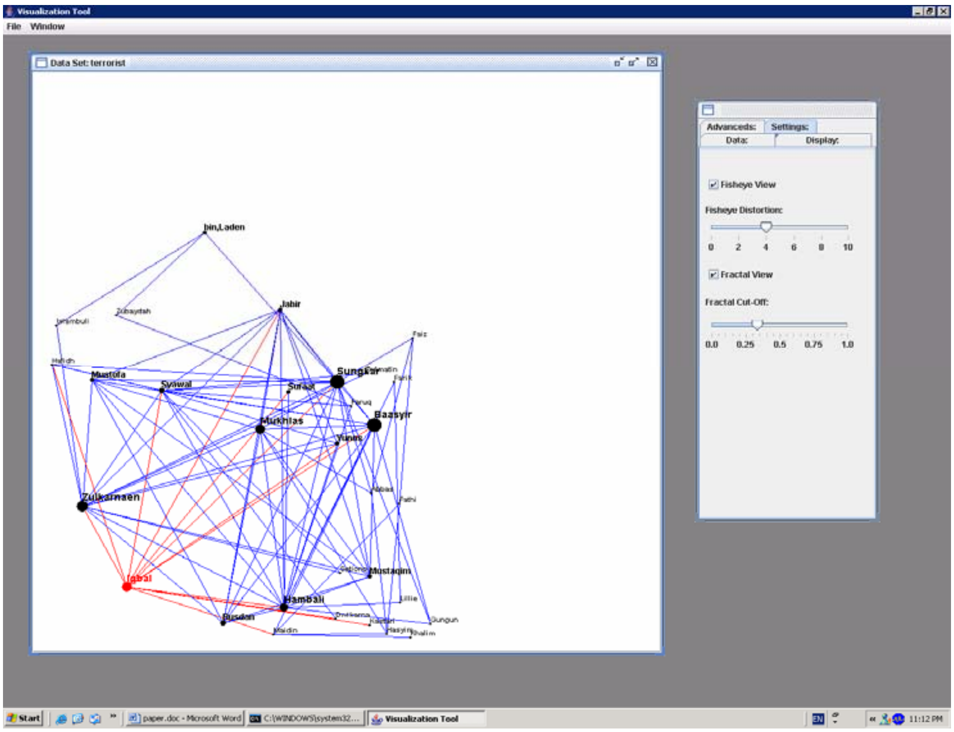


Figure 5: System User Interface

The user interface of the visualization tool (Figure 5) consists of the drawing window (left) and the control panel (right). The drawing window displays the network and allows a user to select/deselect focuses dynamically by clicking the nodes. The control panel comprises 4 panels: Data, Settings, Display and Adanced (Figure 6).

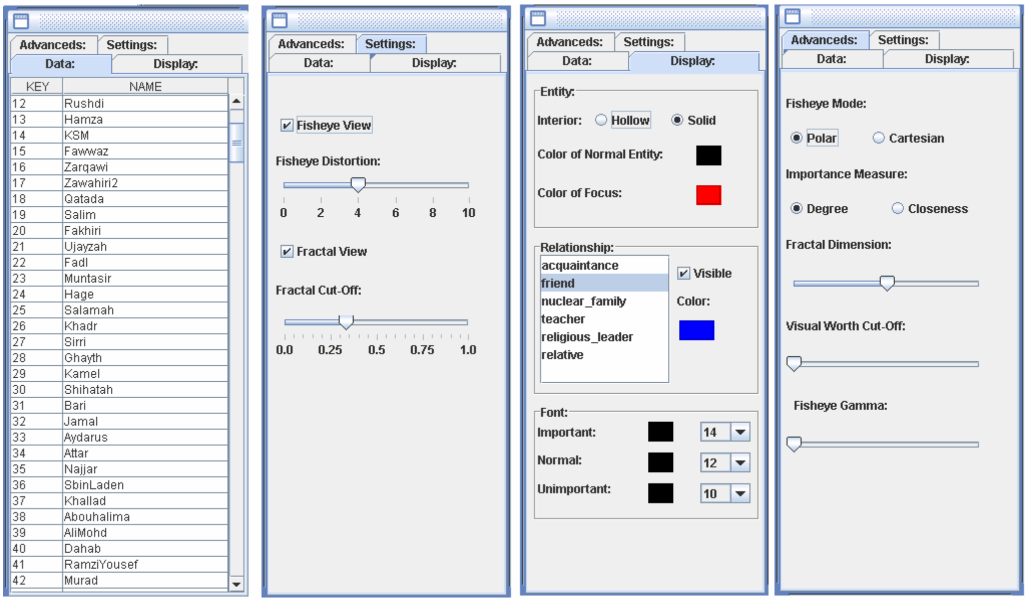


Figure 6: Different Panels of the Control Window

The Data panel lists all the members of the terrorist social network. A user may double click on a particular row of the table to set the corresponding individual as a focus. The Setting panel contains the options for controlling the visualization effect. A user may choose to apply either Fisheye or Fractal view as well as combining the two. The distortion factor and fractal value cut-off are two parameters used to control the degree of magnification and abstraction in fisheye views and fractal views. In the Display panel, a user may set the color and visibility of different types of relationships and font size of node's label. The Advanced panel contains some parameters for sophisticated users who has the advance knowledge in the operation of fisheye views and fractal views, such as the transformation function in fisheye view, the fractal dimension, etc.

5.Case Study

In this section, we present two case studies on how the proposed visualization tools support the analysis of two terrorist cells in the global Salafi jihad network: the plotters of the unsuccessful millennial bombing of the Los Angeles airport and the Hamburg cell responsible for the 9/11 attacks. In particular, we show how the visualization techniques facilitate the exploration of the inner structures of the two terrorist cells, which are originally embedded in the global network. All the background information used in our analysis were detailed in [14].

5.1 The U.S. Millennial Plot

In Figure 7, Fateh Kamel (the focus) was the hub around which the network responsible for millennial plot grew. After applying fisheye views and fractal views (Figure 7 (b)), most of the other important figures related to Fateh are clearly revealed: Omary set up the network of supporters with Fateh for the Bosnia jihad, Atmani and Ouzghar were invited to Canada by Fateh, Ressam carried out the bomb mission and failed.

Ressam and Meskini were the two terrorists who carried out the operation. Ressam attempted to infiltrate from Canada to U.S. but failed. Meskini, who lived in U.S., was supposed to assist Ressam after he crossed the border. After reduction of most less relevant nodes using fractal view and magnification with Fisheye View (Figure 8(b)), an association path between them through Haouari and Fateh is clearly seen. It turns out that Haouari is a childhood friend of Meskini and Meskini also bought Fateh's store from him. Fateh was the leader of the group.

(a) (b)

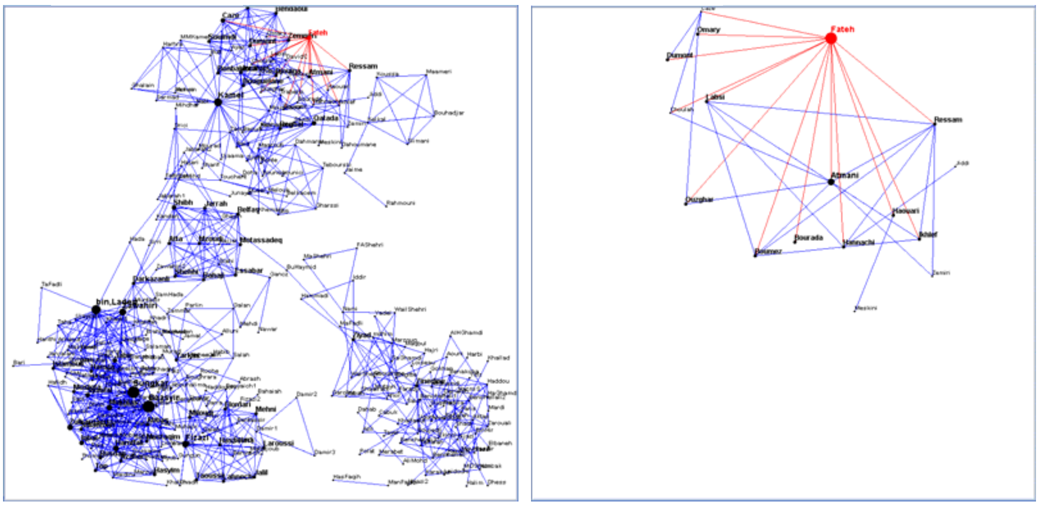


Figure 7: The view of the network with Fateh selected as Focus before and after applying Fisheye and Fractal View

(a) (b)

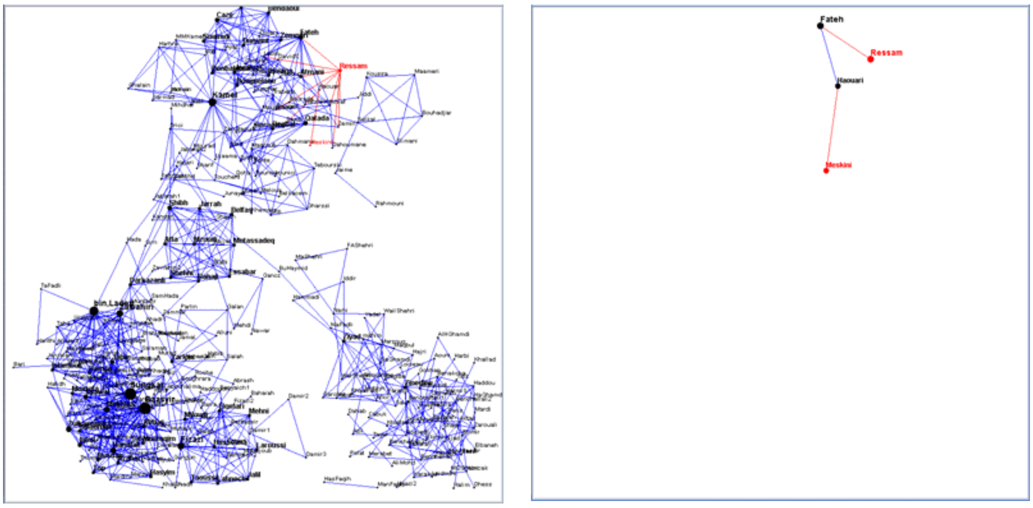


Figure 8: Applying Fisheye and Fractal View to analyze linkages between Ressam and Meskini

5.2 The Hamburg Cell

The Hamburg Cell is a closely tied group, who carried out the 9/11 attack. Of its members, Atta, Jarrah and al-Shehhi received training in the U.S. and carried out the operation. Figure 9 shows the display when selecting these three nodes as focuses.

(a) (b)

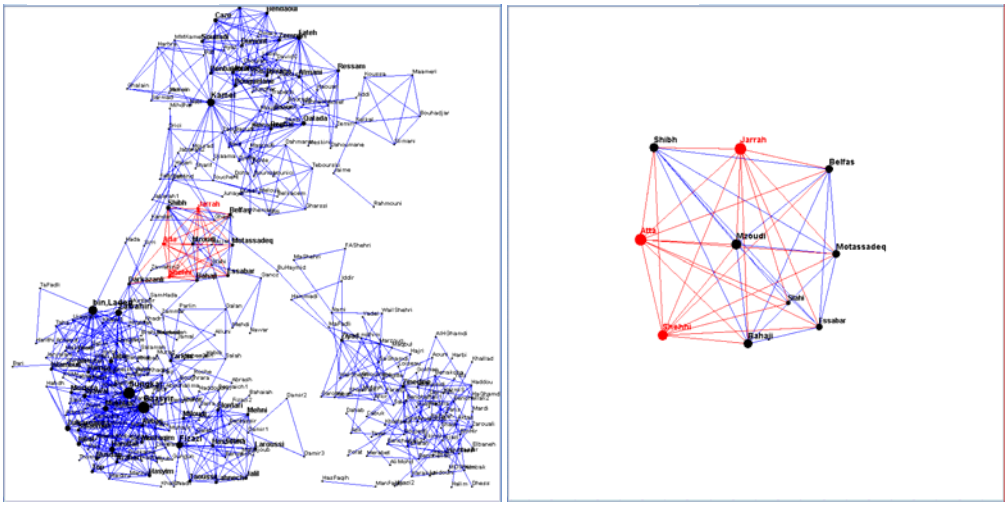
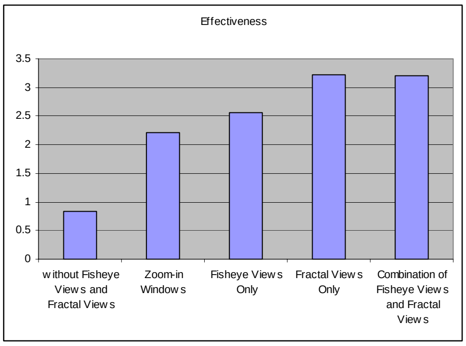


Figure 9: View of the Hamburg Cell

After applying fisheye and fractal View, the inner structure of this group is more clearly shown. Shibh was responsible for coordination while Mzoudi, Motassadeq, Essabar and Bahaji played supporting roles and took care of affairs back in Germany.

6.Experiments

To evaluate the performance of the proposed visualization techniques for the terrorist social networks, we have conducted a user evaluation with ten subjects. Each subject was first given a training session to demonstrate the functionality of the visualization tools and gains hands-on experience with the system. After the training session, the subjects were randomly assigned twenty tasks. The tasks include identifying the key person in the terrorist groups and the interaction patterns of the terrorists, similar to the tasks as presented in the above case studies. For each of the tasks, the subjects were also randomly asked to use the visualization tools without fisheye views and fractal views, with zoom-in windows, with fisheye views only, with fractal views only, or with combination of fisheye views and fractal views. We measure the effectiveness by the number of correct answers a subject provided for the tasks and measure the efficiency by the average time a subject needed to complete the tasks.



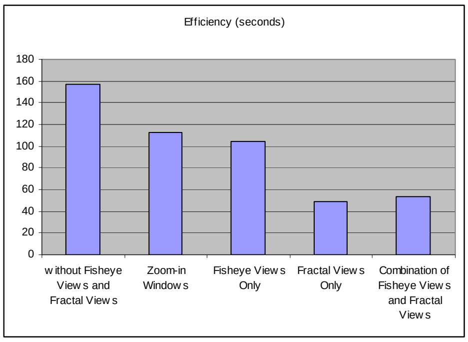


Figure 10: Experimental Results

The experimental results are presented in Figure 10. It is shown that using fractal views only or combination of fisheye views and fractal views obtain the highest effectiveness and efficiency. The effectiveness and efficiency of using fisheye views only is substantially lower than using fractal views only or combination of fisheye and fractal views. However, we only observe substantially higher effectiveness when we compare using fisheye views and using zoom-in windows.

7.Conclusion

In the recent years, we have seen frequent reports of terrorist attacks all around the world. A good understanding of the terrorist organizations and their social networks is helpful to combat the potential terrorist attacks. Visualization tools are capable to support the analysis of terrorist social networks especially when the networks are large and complex. In this work, we have utilized the spring embedded algorithm to initialize the coordinates of nodes in terrorist social networks and applied the fisheye views and fractal views for visualizing and exploring the global Salafi Jihad network interactively. The spring embedded algorithm optimizes the usage of the two dimensional space to display the network. The distance between nodes represents the strength of their associations. The fisheye views are developed based on a distortion approach to magnify the area of interests selected by users. On the other hand, the fractal views are developed based on an information reduction approach to filter the less relevant information from the overloaded visualization space. Combination of these techniques or using fractal views only can effectively and efficiently support users to extract to identify the key persons in the terrorist groups and discovering specific patterns of interaction among the terrorists. Two case studies, the US Millennial Plot and the Hamburg Cell, are presented to demonstrate how the proposed visualization tool to extract and identify the relationship among the key terrorists in these terrorist attacks. The experimental result shows that the combination of fisheye views and fractal views or fractal views alone have the best performance in terms of effectiveness and efficiency.

8. References

[1] M. K. Sparrow: The application of network analysis to criminal intelligence: An assessment of the prospects. in *Social Network*, Vol. 13, 1991

[2] J. S. Mcillwain: Organized crime: a social network approach. *Crime, Law & Social Change*, Vol. 32, 1999

[3] D. Ronfeldt, J. Arquilla, "What next for networks and netwars?" *Networks and Netwars: The Future of Terror, Crime and Millitancy*. Rand Press, 2001

[4] S. Wasserman, K. Fause, "Social Network Analysis: Methods and Applications", Cambridge, Cambridge University Press, 1994

[5] J. Xu, B. Marshall, S. Kaza, and H. Chen, "Analyzing and Visualizing Criminal Network Dynamics: A Case Study" in *Proceedings of the 2nd NSF/NIJ Symposium on Intelligence and Security Informatics* (*ISI'04*), Tucson, AZ, June 10-11, 2004.

[6] J. Xu and H. Chen, "Criminal Network Analysis and Visualization," *Communication of the ACM*, 48(6), 2005, pp. 101-107.

[7] J. Xu and H. Chen, "CrimeNet Explorer: A Fremework for Criminal Network Knowledge Discovery," *ACM Transactions on Information Systems*, 23(2), April, 2005, pp. 201-226.

[8] P. Eades, "A Heuristic for Graph Drawing". In *Congressus Numerantium*, Vol. 42, 1984

[9] J. Assa, D. Cohen-Or, T. Milo, "Displaying Data in Multidimensional Relevance Space with 2D Visualization Maps", in *Proceedings of IEEE Conference on Visualization,* 1997

[10] G.W. Furnas, "Generalized Fisheye Views", in Proceedings of the SIGCHI Conference on Human Factors in Computing System, 1986

[11] S. Manojit, M.H Brown, "Graphical Fisheye Views", in *Communications of the ACM*, Vol. 37, 1994

[12] H. Koike, "Fractal Views: a Fractal-based Method for Controlling Information Display" in *ACM Transactions on Information Systems* Vol. 13 (3), 1995

[13] J. Feder, "Fractals", Plenum, New York, 1988

[14] M. Sageman, "Understanding Terror Networks", University of Pennsylvania Press, 2004

[15] T.H. Cormen, C.E. Leiserson, R.L. Rivest, and C. Stein, "Introduction to Algorithms, 2nd Edition", Mcgraw-Hill, 2002

[16] H. Chen, K.J. Lynch, "Automatic Construction of Networks of Concepts Characterizing Document Databases", *IEEE Transactions on Systems, Man and Cybernetics* Vol. 22(5) 1992

[17] Y. K. Leung and M. D. Apperley, "A review and taxonomy of distortion-oriented presentation techniques", *ACM Transactions on Computer-Human Interaction (TOCHI)*, 1(2) 1994

[18] C. C. Yang, H. Chen, and K. Hong, "Visualization of Large Category Map for Internet Browsing," *Decision Support Systems, Special Issue on Web Retrieval and Mining*, vol.35, no.1, April, 2003, pp.89-102

[19] C. C. Yang, H. Chen, and K. Hong, "Exploring the World Wide Web with Self-Organizing Map," *Proceedings of the International World Wide Web Conference*, Honolulu, Hawaii, May 7-11, 2002